CM-400-427-01

DII.3200.Sol251.Kernel.P2.UM-1

Defense Information Infrastructure (DII)

Common Operating Environment (COE)

User's Manual (UM) for
Kernel Version 3.2.0.0 Patch 2 Security Administration
(Solaris 2.5.1)

Version 1.0

November 18, 1997

Prepared for:

Defense Information Systems Agency

Prepared by:

Inter-National Research Institute (INRI)
12200 Sunrise Valley Drive, Suit 300
Reston, Virginia 20191

Table of Contents

1. Scope 1
1.1 Identification 1
1.2 System Overview 1

2. Referenced Documents 3

3. Software Summary 5
3.1 Software Description 5
3.1.1 Local and Global User Accounts 6
3.1.2 Global and Local Profiles 6
3.1.3 Accounts and Profiles Interaction 7
3.1.4 Default Profile 7
3.1.5 Safe Profile 8
3.2 Software Inventory 8
3.3 Software Environment 9
3.4 Software Organization and Operation Overview 9
3.5 Modes of Operation 10
3.6 Security and Privacy 10
3.7 Assistance and Problem Reporting 10

4. Access to the Software 13
4.1 Software Setup 13
4.1.1 System Configuration 14
4.1.2 Differences Between NIS and NIS+ 14
4.1.3 Security Manager Configuration File 15
4.1.4 Familiarization 16
4.1.4.1 Security Manager Catalog Basics 17
4.1.4.1.1 Selecting Scope 17
4.1.4.1.2 Resizing the Columns 18
4.1.4.1.3 Reordering Columns 18
4.1.4.1.4 Sorting Contents by Column 18
4.1.4.1.5 Adding Entries to a Catalog 18
4.1.4.1.6 Modifying Entries in a Catalog 18
4.1.4.1.7 Deleting Entries from a Catalog 19
4.1.4.2 Security Manager Pull-Down Menus 19
4.1.4.2.1 File Menu 19
4.1.4.2.2 Edit Menu 20
4.1.4.2.3 View Menu 20
4.1.5 Access Control 21
4.1.6 Installation and Configuration 21
4.2 Initiating a Session 21
4.3 Stopping and Suspending Work 23

Table of Contents (continued)

5. DII COE Security Administration Processing Guide 25
5.1 Capabilities 26
5.2 Conventions 26
5.3 Processing Procedures 27
5.3.1 Assigning Passwords 28
5.3.2 Modifying Profiles 31
5.3.3 Unlocking Users 35
5.3.4 Monitoring Hard Disk Capacity 38
5.3.5 Managing the Audit Log Files 40
5.3.5.1 Monitoring the Audit Log Files 40
5.3.5.2 Manually Deleting Audit Log Files 43
5.3.6 Maintaining User Accounts 45
5.3.6.1 User Catalog 46
5.3.6.2 Creating Accounts 47
5.3.6.3 Modifying an Account 49
5.3.6.4 Deleting an Account 51
5.3.7 Maintaining Profiles 51
5.3.7.1 Profile Catalog 52
5.3.7.2 Creating Profiles 53
5.3.7.3 Modifying Profiles 55
5.3.7.4 Deleting Profiles 56
5.3.8 Viewing the Application Catalog 56
5.3.9 Maintaining UNIX Groups 58
5.3.9.1 UNIX Group Catalog 59
5.3.9.2 Creating UNIX Groups 60
5.3.9.3 Modifying UNIX Group Names 61
5.3.9.4 Deleting UNIX Groups 61
5.3.10 Changing the secman Password 62
5.4 Related Processing 63
5.4.1 Assign or Unassign Users to Profiles 64
5.4.2 Assign or Unassign Applications to Profiles 64
5.5 Data Backup 64
5.6 Error Recovery 65

List of Figures

Figure 1. Example Catalog 17
Figure 2. EM Security Manager Menu Bar 19
Figure 3. Security Manager Window File Menu 19
Figure 4. Security Manager Window Edit Menu 20
Figure 5. Security Manager Window View Menu 20
Figure 6. DII COE Login Screen 22
Figure 7. EM Security Manager Main Window 23
Figure 8. Assign Passwords Window (Sorted by User Name) 29
Figure 9. Assign Passwords Window (Sorted by User ID) 29
Figure 10. Set Password Window 30
Figure 11. Verify Password Window 30
Figure 12. USER PROFILES Window 31
Figure 13. EDIT PROFILE Window 32
Figure 14. EDIT PERMISSIONS Window 33
Figure 15. EDIT MENU ACCESS Window 34
Figure 16. User Account Information Window 36
Figure 17. User Account Information Window with User Account Information 37
Figure 18. Audit Log File Manager Window 39
Figure 19. File(s) to Monitor Window 41
Figure 20. File(s) to Delete Window 44
Figure 21. User Catalog 46
Figure 22. New User Dialog Window 47
Figure 23. Password Mismatch Dialog 48
Figure 24. Modify User Dialog Window 50
Figure 25. Delete Account Dialog 51
Figure 26. Profile Catalog 52
Figure 27. New Profile Window 53
Figure 28. Modify Profile Dialog Window 55
Figure 29. Delete Profile Dialog 56
Figure 30. Application Catalog 57
Figure 31. Unix Group Catalog 59
Figure 32. New Unix Group Dialog 60
Figure 33. Modify Unix Group Dialog 61
Figure 34. Delete Group Dialog 61
Figure 35. Set Password Window 62
Figure 36. New Password Window 63

This page intentionally left blank.

1. Scope

1.1 Identification

This document provides information needed for using the Defense Information Infrastructure (DII) Common Operating Environment (COE) Kernel Version 3.2.0.0 security administration capabilities for Sun hardware running the Solaris 2.5.1 Operating System. See the *DII COE Integration and Runtime Specification* for more information about the DII COE. See the *DII COE Installation Procedures for the Kernel* for more information about installing the DII COE kernel and segments.

The DII COE Kernel is a Government off-the-shelf (GOTS) package that includes both GOTS and Commercial off-the-shelf (COTS) software, as described in Section 1.2, *System Overview.*

> **NOTE:** Throughout this document, `Courier` font is used to indicate entries to be typed at the keyboard, UNIX commands, file and directory names, and screen text. For example:
>
> The file is located in the `DII_DEV` directory.

> **NOTE:** Throughout this document, any mention of the *Security Manager* refers to a function within the overall Security Administration software. Information about the Security Manager does not necessarily apply to general security administration. The text notes wherever any information about the Security Manager might be confused with the Security Administration software. The Security Manager is accessed through an icon in the `L:SSO_Default` window.

1.2 System Overview

The DII COE will normally make available a large number of segments, not all of which are required for every application. The DII COE Kernel is the minimum set of software required on every workstation regardless of how the workstation will be used. These components include the operating system and windowing services, as well as external environment interfaces. The DII COE Kernel for Solaris 2.5.1 includes the following components:

- System Administration function
- Security Administration function
- Runtime tools
- COTS software (windowing environment)
- GOTS software.

The Security Administration function described in this manual provides the ability for authorized users to create, delete, and maintain user accounts and UNIX groups, as well as to define *profiles*, which provide users with easy access to the executables and icons they need to perform their duties. Profiles provide a mechanism by which a security administrator can group sets of users, often by their job responsibilities, to appropriate applications.

2. Referenced Documents

The following documents are referenced in this guide:

- DII COE I&RTS:Rev 2.0, *Defense Information Infrastructure (DII) Common Operating Environment (COE) Integration and Runtime Specification (I&RTS)*, Version 2.0, October 23, 1995

- DII COE I&RTS:Rev 3.0, *Defense Information Infrastructure (DII) Common Operating Environment (COE) Integration and Runtime Specification (I&RTS)*, Version 3.0, January 1997

- DII.3200.Sol251.Kernel.IG-1, *Defense Information Infrastructure (DII) Common Operating Environment (COE) Version 3.2.0.0 Kernel Installation Guide (Solaris 2.5.1)*, July 25, 1997

- DII.3200.Sol251.Kernel.P2.IP-1, *Defense Information Infrastructure (DII) Common Operating Environment (COE) Installation Procedures (IP) for Kernel Version 3.2.0.0 Patch 2 (Solaris 2.5.1)*, November 18, 1997

- DII.3200.Sol251.AG-1, *Defense Information Infrastructure (DII) Common Operating Environment (COE) Version 3.2.0.0 System Administrator's Guide (Solaris 2.5.1)*, July 25, 1997

- TED002004000, *TriTeal Enterprise Desktop (TED™) Version 4.0 User's Guide*, TriTeal Corporation, Carlsbad, CA, August 1995

- DII UIS V3.0 Draft, *User Interface Specifications for the Defense Information Infrastructure (DII)*, Version 3.0 Draft, September 1997.

This page intentionally left blank.

3. Software Summary

This following sections provide a summary of the Security Administration function of the DII COE Kernel.

The following paragraph applies to the Security Manager and not to the general Security Administration software.

The `Security Manager` provides the ability for authorized users to create, delete and maintain user accounts and UNIX groups, as well as define *profiles* that provide users with easy access to the executables and icons they need to perform their duties. A *profile* provides a mechanism by which a security administrator can group sets of users, often by their job responsibilities. Rather than assigning each user a list of applications they are allowed to access, the security administrator can define a profile which provides convenient access to a series of applications, and then assign users to one or more profiles. For example, the security administrator may create a profile called `GCCS User`, which would contain all of the applications that a typical Global Command and Control System (GCCS) user would need to access. The administrator could then assign this profile to one or more user accounts. Similarly, the administrator could create a profile called `Backup` that would provide access to the applications needed to perform a system backup. This profile could again be assigned to one or more user accounts. Security Manager requires that users have at least one profile assigned to them.

3.1 Software Description

The DII COE is a core or minimum set of software components required on every workstation to support mission applications. The components include the operating system and windowing services, as well as external environment interfaces. Another of these components is the Security Administration component, or segment. When combined with the operating system, the Security Administration segment gives the security administrator the ability to enforce system security policy.

The Security Administration component provides the capability to establish, maintain, and delete user accounts and UNIX groups and define profiles. These profiles, based upon definition, provide users with levels of access to executable applications with menus and icons that they need to perform their duties.

An improvement with the delivery of the DII COE Kernel 3.2 Patch 2 release is the ability to monitor and manage the growth of the audit logs. The audit logs retain information on user logins and logouts to the system. This improvement will provide notification of the growth of these files as well as manual or automatic removal of these files when thought necessary by the security administrator.

The Security Administrator account group serves as a template for establishing a runtime environment for the security administrator. It contains template files for specifying COE processes to launch at login time, functions to be made available to operators, and global default preferences such as color selections for window borders.

Once profiles have been created and defined, use the `Edit Profiles` icon to modify profiles to add and restrict access to functions that have menus and options.

The following paragraph and the remainder of Section 3.1 apply to the Security Manager and not necessarily to the general Security Administration software.

Security Manager supports both local and global user accounts and local and global profiles. You should establish whether or not your site will be using local and global user accounts and profiles before you begin using Security Manager. Local and global accounts and local and global profiles can exist simultaneously.

3.1.1 Local and Global User Accounts

Local user accounts are created and maintained on an individual machine and allow the user to log in only on that machine. Global accounts use network services, such as Network Information Service (NIS) and Network File System (NFS), to create and maintain accounts that allow a user to log in to multiple machines using the same password and account.

If a user is created with a *local* scope, then:

C The User Account data is stored in `/etc/passwd`.

C Their UNIX Group memberships are stored in `/etc/group`.

C Their User Directory is located at `/h/USERS/local/<login-name>`.

If a user is created with a *global* scope, then:

C The User Account data is stored in the NIS or NIS+ `passwd` database.

C Their UNIX Group memberships are stored in the NIS or NIS+ group database.

C Their User Directory is located at `/h/USERS/global/<login-name>`.

3.1.2 Global and Local Profiles

Global user accounts are available based on the configuration of NIS or NIS+ on the system. Global user accounts will be disabled on a standalone workstation. On a NIS client, global user accounts will be available for viewing, but modifying the accounts or groups is not allowed. On a NIS or NIS+ server, or a NIS+ client added to the administration group, full global account functionality is available.

Similarly, local profiles are defined on, and available to, the local machine, whereas global profiles are defined once, but made available to a number of machines via an NFS mount point.

If the profile's scope is local, all of the information about the profile is stored in the local machine's user-profile database at `/h/USERS/local/Profiles`. If the profile's scope is global, all of the information about the profile is stored on another machine and served by NFS. The global profile's information should be mounted so it is at `/h/USERS/global/Profiles` on all client machines.

Local profiles are always available on all machines.

3.1.3 Accounts and Profiles Interaction

The Security Manager provides the tools to allow a site's security administrator to associate users with profiles. The Security Manager allows local users to be associated with both local and global profiles. It also allows global users to be associated with both local and global profiles. *It is recommended that all users be assigned to at least one local profile*, as this will allow the user to access applications even if the NFS or NIS server is unavailable due to failure or network segmentation.

3.1.4 Default Profile

In the 3.0 version, a user's default profile only established their default group (i.e., the GID that appears in either the `/etc/passwd` file or the NIS/NIS+ `passwd` entry); it did *not* add the user to the profile. The default group assigned was derived from the UNIX group assigned to the account group to which the default profile belongs.

However, in the 3.2 version, assigning a user to a default profile not only assigns the user's default group ID (GID) in the manner previously discussed, but also adds the user to that profile. There are some subtle points for this assignment.

C Changing a user's default GID once it has been assigned can be very problematic since it may involve changing the group ownership of the user's files, which may be scattered in various directories. Therefore, the decision was made *not* to allow a user's GID to be changed by Security Manager once it has been created.

C Although the user's default profile will appear in the profile's window, it should not be removed from the user or deleted. Attempting to unassign users from their default profiles will result in an `invalid data` error, and Security Manager will not allow the change to be made.

3.1.5 Safe Profile

The concept of a safe profile has been incorporated into the Security Manager. The intent is to provide a fail-safe profile that is always available. When a user logs on, the session manager automatically tries to resume the user's previously assumed profiles. If they are all unavailable because they have been deleted or others are using them while locking is enabled, the session manager will look at the user's profile, and if the safe profile has been assigned but not previously assumed by the user, it will try to assume the safe profile. Failing this, the session manager will log the user in with *no* profiles. The safe profile has the same capabilities as any other profile.

There are a few subtle points concerning safe profiles.

C The security administrator must create the safe profile using Security Manager.

C The safe profile should ideally be a local profile, but it may be global as well.

C The session manager will not try to assume the safe profile upon failure of the user's previously assumed profiles unless the safe profile is assigned to the user.

C The safe profile should never be locked.

C The safe profile must actually be named `Safe Profile`. Because profile names must be unique within a scope, one safe profile defined within a scope can exist.

3.2 Software Inventory

The following section lists the directory structure and software files that make up the Security Administration account.

```
/h/AcctGrps/SecAdm:
   Scripts
   SegDescrip
   bin
   data

/h/AcctGrps/SecAdm/Scripts:
   .Xdefaults
   .Xdefaults.SSO
   .cshrc
   .cshrc.SSO
   .login
   .mwmrc.runtime
   .xsession
   .xsession.SSO
   RunSSO

/h/AcctGrps/SecAdm/SegDescrip:
   FileAttribs
   Installed
   PostInstall
```

```
      ReleaseNotes
      SegInfo
      SegName
      VERSION

   /h/AcctGrps/SecAdm/bin:
      SSOEditProfiles

   /h/AcctGrps/SecAdm/data:
      Icons

   /h/AcctGrps/SecAdm/data/Icons:
      SecIcons
```

The Security Manager application and associated user-profile database are automatically installed as part of the DII COE Kernel load. If global accounts are being used, NIS or NIS+ must be properly installed and configured.

3.3 Software Environment

The following resources are needed to install and operate the DII COE Security Administration software:

C A Sun computer

C Solaris 2.5.1 Operating System

C DII COE Kernel Version 3.2.0.0 (Solaris 2.5.1)

C *DII COE Kernel Installation Guide*

C *DII COE Installation Procedures for the Kernel Patch 2*

C *DII COE System Administrator's Guide*

For the Security Manager, if your site will be using global user accounts, NIS or NIS+ must be set up and configured properly. See Section 4.1 for a detailed discussion on how to configure NIS and the Security Manager for your site.

3.4 Software Organization and Operation Overview

The Security Administrator account group serves as a template for establishing a runtime environment for the security administrator. It contains template files for specifying COE processes to launch at login time, functions to be made available to operators, and global default preferences such as color selections for window borders.

Once profiles have been created and defined, use the `Edit Profiles` icon to modify profiles to add and restrict access to functions that have menus and options.

The following applies to the Security Manager and not necessarily to the general Security Administration software.

The Security Manager interface revolves around catalogs or windows. One catalog exists for each of the four main types of objects you will need to administer: users, profiles, applications, and UNIX groups. Only one catalog can be active, or visible, at a time. Each catalog provides the tools that allow you to view, create, modify, or delete objects.

In general, you will begin security administrator activities by activating the appropriate catalog and then interacting with the catalog using the functions provided with the three pull-down menus, or through interface short-cuts, such as double-clicking on an entry to modify it. For example, to add a new user, bring up the User Catalog and use the `New User` option provided under the `File` menu to enter detailed information for the new account.

3.5 Modes of Operation

The Security Administration segment and its capabilities are available only to those users that have been given access by the security administrator through definition of a profile and subsequent assignment of that profile to a user account.

3.6 Security and Privacy

Copyright, Inter-National Research Institute, Inc. 1997, All Rights Reserved. This material may be reproduced by or for the U.S. Government pursuant to the copyright license under the clause at DFARS 252.227-703 (OCT 1988). No other licenses are required for using this software. No freeware or shareware is included. Because this software is unclassified, no security considerations apply.

3.7 Assistance and Problem Reporting

To receive immediate assistance with a problem or to report a problem, call the DII COE Hotline at (703) 735-8681 (DSN 653-8681) between the hours of 9:00 A.M. and 5:00 P.M. Eastern Standard Time. You can also send a facsimile to (703) 735-3080 (DSN 653-3080), send an e-mail message to hotlinec@ncr.disa.mil, or look on the DII COE Hotline web site at the following URL: http://spider.osfl.disa.mil/dii/hotline/index.html. The DII COE Hotline is located at the Operational Support Facility (OSF) in Sterling, Virginia.

If a problem cannot be corrected by the procedures described in this document, follow these guidelines to report it:

STEP 1: **Make sure the problem can be repeated**.

STEP 2: **Record pertinent information**. Record the problem, the last steps leading to the problem, and the frequency with which the problem occurs.

STEP 3: **Describe attempts to solve the problem**.

This page intentionally left blank.

4. Access to the Software

> **NOTE:** Throughout this manual, it is assumed that you are modifying local accounts and profiles, as designated by options beginning with `L:`. To modify global accounts and profiles, use options beginning with `G:` instead.

The following procedure applies to the Security Manager and not to the general Security Administration software.

Only those user accounts assigned to profiles under the Security Administrator account group may run Security Manager. Follow the steps below to access the Security Manager.

STEP 1: **Log in as `secman`**.

STEP 2: **Enter the appropriate password**.

STEP 3: **Double-click the `Application Manager` icon on the CDE Main Control Panel**. Refer to the *TriTeal Enterprise Desktop User's Guide* for more information about CDE.

STEP 4: **Double-click the `DII_APPS` icon**. The `Application Manager - DII_APPS` window appears.

STEP 5: **Double-click the `L:SSO_Default` icon**. The `Application Manager - L:SSO_Default` window appears.

STEP 6: **Double-click the `Security Manager` icon**. The `Security Manager` window appears.

This section provides procedures for accessing the DII COE Security Administration software.

4.1 Software Setup

This section gives procedures to install, deinstall, configure, and access the DII COE Security Administration software.

The following paragraph applies to the Security Manager and not to the general Security Administration software.

The behavior of the Security Manager application depends on both the system's configuration (i.e., which network services are available and how they are configured) and the settings defined in Security Manager's own configuration file.

4.1.1 System Configuration

Section 4.1.1 applies to the Security Manager and not necessarily to the general Security Administration software.

Workstations can be configured as standalone workstations. Standalone workstations can only have local accounts and profiles. A network information service, NIS or NIS+, must be operating on the workstations to support global accounts and a network file system (such as NFS) must be running to support the serving of global profiles.

HP-UX workstations can act as NIS clients or NIS servers. Solaris workstations can act as NIS clients, NIS+ clients, or NIS+ servers. A Solaris workstation configured as a NIS+ server must run in YP compatibility mode to support NIS clients. A Solaris workstation configured as a NIS+ client requires another Solaris workstation configured as a NIS+ server.

4.1.2 Differences Between NIS and NIS+

Section 4.1.2 applies to the Security Manager and not necessarily to the general Security Administration software.

Under NIS, client workstations do not have the ability to alter the NIS database on the server. Under NIS+, which is for Solaris only, if a client NIS+ workstation and NIS+ user are both members of the NIS+ administration group, that user/workstation combination can change the NIS+ database on the server. These restrictions are extended to Security Manager when dealing with global accounts, or those accounts served by NIS or NIS+.

Security Manager executing on a NIS client can view global user accounts. All options to modify UNIX accounts and groups will be disabled. Profile management will still be available for global profiles, as well as all local functionality.

Follow the steps below to add an existing NIS+ client workstation to the NIS+ administration group.

STEP 1: **Log in to the NIS+ server as a user who is already a member of the NIS+ administration group**.

STEP 2: **Bring up a terminal window**.

STEP 3: **Type the command to add the workstation**. Enter the following command on the command line:

```
% nisgrpadm -a admin.<domain>. <client_workstation>.<domain>.
```

STEP 4: **Check status message for success**.

STEP 5: **Suppy the login password**. Any account with administrative privileges on a NIS+ workstation must go through an additional step of supplying the login password when invoking Security Manager. When Security Manager is launched from the icon, a dialog will prompt for the login password and a confirmation password. If the account does not have the proper privileges, or the password is incorrect, an error dialog displays an error message.

> **NOTE:** As discussed in Section 5.4.1, *Assign or Unassign Users to Profiles*, a profile directive is provided to automatically add or delete a user from the NIS+ administration group when the user is assigned or unassigned from an administrative profile. Administrative profiles are listed in the file `/h/AcctGrps/SecAdm/admin/scripts/admin_profiles`.
>
> This file is modifiable by any user in the UNIX group `admin` and should be modified to contain a list of profiles to be assigned to users with system administration duties.

4.1.3 Security Manager Configuration File

Section 4.1.3 applies to the Security Manager and not necessarily to the general Security Administration software.

The default behavior of Security Manager can be modified by changing the parameters stored in the `/h/AcctGrps/SecAdm/data/config/secman_defaults` configuration file. This file is an ASCII file, changeable only by the super-user. Values in the file appear one per line, starting with the identifier, a colon, then the value being assigned to the identifier. They are as follows:

- `default_profile_local:<Account Group>:<Profile Name>`

  The value assigned to this token appears as the default profile for creating new local accounts. The value must match an existing local profile and account group.

- `default_profile_global:<Account Group>:<Profile Name>`

  This value assigned to this token appears as the default profile for creating new global accounts. It is the only token in `secman_defaults` not specified when the workstation is installed. The value must match an existing global profile and account group.

- `uid_min_local:<integer> uid_max_local:<integer>`

  These two tokens are used to define a range of valid user ID numbers that are permitted for local accounts. Security Manager will not allow local user accounts to be created with ID numbers outside of this range.

- `uid_min_global:<integer> uid_max_global:<integer>`

These two tokens are used to define a range of valid user ID numbers that are permitted for global accounts. Security Manager will not allow global user accounts to be created with ID numbers outside of this range.

C `gid_min_local:<integer> gid_max_local:<integer>`

These two tokens are used to define a range of valid group ID numbers that are permitted for local groups. Security Manager will not allow local groups to be created with ID numbers outside of this range.

C `gid_min_global:<integer> gid_max_global:<integer>`

These two tokens are used to define a range of valid group ID numbers that are permitted for global groups. Security Manager will not allow global groups to be created with ID numbers outside of this range.

C `nis_path:<directory_path`

This token is used to define the location of the source files used to populate the NIS (not NIS+) database. This token is not referenced on workstations using NIS+.

C `modify_accounts:<true|false>`

This token, when defined as true, allows Security Manager to modify the UNIX user accounts and groups. It should be set to false when other means of manipulating accounts and groups are in use. Regardless of the setting of `modify_accounts`, Security Manager will be able to perform profile management.

The numeric ranges specified for user and group IDs based on scope are recommended not to overlap, helping to prevent possible ownership conflicts and data loss. In addition, it makes account and group scope readily identifiable.

4.1.4 Familiarization

For familiarization with operating the software, see the *DII COE System Administrator's Guide*.

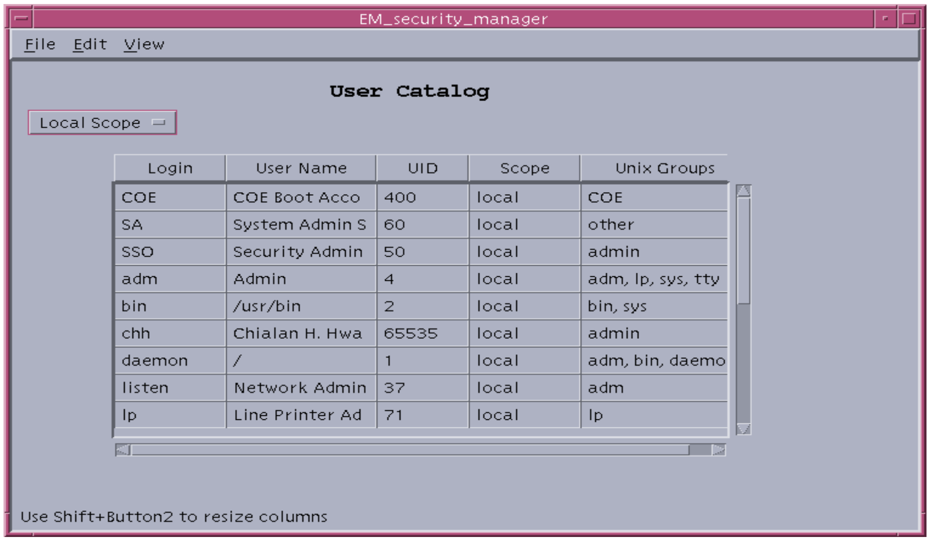
The following paragraph and the remainder of Section 4.1.4 apply to the Security Manager and not necessarily to the general Security Administration software.

The Security Manager interface is comprised of a series of catalogs and pull-down menus. A brief overview of how to work with each of the catalogs is provided below. The detailed functions of each catalog and menu are provided in Section 5.

4.1.4.1 Security Manager Catalog Basics

The Security Manager divides its functions among four different catalogs, each responsible for a particular type of data. Currently, there are catalogs for users, profiles, applications, and UNIX groups. You can interact with only one catalog at a time and use the `View` pull-down menu to specify which catalog to use.

Each of the catalogs has the same basic interface and allows you to perform similar functions. The following sections briefly describe the main functions available from each of the catalogs. Use the catalog displayed in Figure 1 as a reference.



User Catalog

Login	User Name	UID	Scope	Unix Groups
COE	COE Boot Acco	400	local	COE
SA	System Admin S	60	local	other
SSO	Security Admin	50	local	admin
adm	Admin	4	local	adm, lp, sys, tty
bin	/usr/bin	2	local	bin, sys
chh	Chialan H. Hwa	65535	local	admin
daemon	/	1	local	adm, bin, daemo
listen	Network Admin	37	local	adm
lp	Line Printer Ad	71	local	lp

Use Shift+Button2 to resize columns

Figure 1. Example Catalog

4.1.4.1.1 Selecting Scope

Each catalog has a `Scope` pull-down menu that determines the scope of the data displayed in the catalog. A scope may be

C Local, which indicates that only user, profile, group and application information stored locally on this machine should be displayed

C Global, which indicates that the information being displayed is being served by a network service (i.e., NIS & NFS)

C Both, indicating that both local and global sources should be displayed.

Choose whichever scope is appropriate for your work. Each catalog may have a different scope. If multiple scopes are active, then the values stored in significant fields will be prefaced by either an `L:` or a `G:` indicating that the entry is either local or global respectively.

NOTE: Accessing global data is somewhat slower than accessing local data and may be impacted by network load and connectivity.

4.1.4.1.2 Resizing the Columns

Occasionally, a catalog will contain more data than can be displayed on a single screen. In this case, horizontal or vertical scrollbars will appear, and you may use these scrollbars to make additional information visible.

The columns of each of the catalogs are set to a predefined width. You may resize columns by:

1. Positioning your cursor over the boundary between two columns *in the body of the catalog,* not the header.

2. Holding down the shift-key and clicking and holding down the second mouse button.

3. Dragging the column to its desired size.

NOTE: Because Security Manager is likely used by several people, it will not retain your changes.

4.1.4.1.3 Reordering Columns

This version of Security Manager does not provide the user with the ability to reorder columns.

4.1.4.1.4 Sorting Contents by Column

You can sort the catalog in ascending order based on the contents of any of the columns. To sort a catalog, place the cursor over the column heading you want to sort and click the left mouse button. Currently, no provision exists for sorting multiple columns simultaneously.

4.1.4.1.5 Adding Entries to a Catalog

To add an entry, use the `File` pull-down menu. At this time, the catalog does not provide a short cut for adding entries.

4.1.4.1.6 Modifying Entries in a Catalog

You may directly access the modify screen for a given entry by double-clicking the entry. For example, from the User Catalog, double-click an entry to automatically bring up the `Modify User` screen containing data from that record.

4.1.4.1.7 Deleting Entries from a Catalog

To delete an entry in a catalog, highlight the desired entry and select the appropriate `Delete` option from the `Edit` pull-down menu. For example, to delete a user's account, bring up the user catalog, highlight the user's entry, and choose `Delete User` from the `Edit` pull-down menu. A dialog box asks you to confirm deletion of this user’s account.

4.1.4.2 Security Manager Pull-Down Menus

The Security Manager application window (Figure 2) contains a menu bar with three pull-down menus. Use these menus to access almost all of Security Manager's functions. In each of these menus, some options will appear grayed out, showing that the option is either not yet implemented or inappropriate at the moment. Each of the menus will be discussed below.

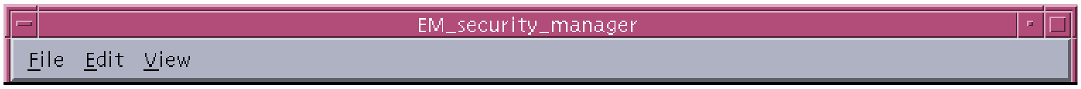


Figure 2. EM Security Manager Window Menu Bar

4.1.4.2.1 File Menu

The `File` menu (see Figure 3) provides the ability to create new user, profile, or UNIX group entities and to exit the Security Manager application. Many of the other features on the `File` menu are grayed out, indicating that the ability to print reports, import users and profiles from another machine, export users and profiles from this machine, and to temporarily disable user accounts will be provided in future Security Manager releases.

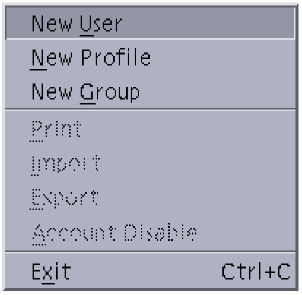


Figure 3. Security Manager Window File Menu

Pull-down menu functions are only active when their associated catalog is active. For example, when the User Catalog is active, the `File` menu will provide options for `New User` and `Exit`. The options for `New Profile` and `New Group` are only available when you are using the Profile Catalog or UNIX Group Catalog respectively.

4.1.4.2.2 Edit Menu

The `Edit` menu (see Figure 4) provides the ability to modify or delete existing user, profile, or UNIX group entities. The `Clear`, `Copy`, and `Paste` features are reserved for future use and will be used extensively in the matrix operations that are part of the next `Security Manager` release.

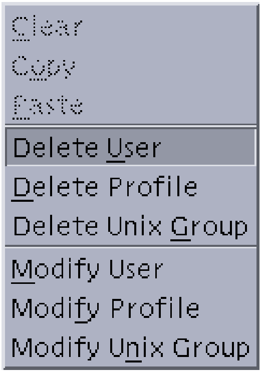


Figure 4. Security Manager Window Edit Menu

Pull-down menu functions are only active, not grayed out, when their associated catalog is active. For example, when the User Catalog is active, the `Edit` menu will provide options for `Delete User` and `Modify User`. The options for deleting and modifying profiles and UNIX groups are available only when you are using the Profile Catalog or UNIX Group Catalog respectively.

4.1.4.2.3 View Menu

The `View` menu (see Figure 5) provides the ability to switch between the four primary catalogs: `User`, `Profile`, `Applications`, and `UNIX Groups`. Choosing one of these options will cause the selected catalog to appear in the `Security Manager` main window.

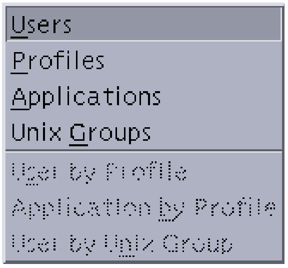


Figure 5. Security Manager Window View Menu

The next release of Security Manager will provide the ability to view and interact with data in a matrix format and will provide three new catalogs. The `User by Profile` catalog will list users on one axis and the available profiles on the other. This will provide an easy way to see which users are assigned to which profile, and to compare two users to see how their access permissions differ. Similarly, the `Application by Profile` catalog will enable applications to easily be assigned to profiles, as well as provide an easy way to view a listing of which applications are assigned to which profiles.

4.1.5 Access Control

This section provides an overview of user security features.

To add passwords, see Section 5.3.1, *Assigning Passwords*. To change the Security Administration password, see Section 5.3.10, *Changing the secman Password*.

The following paragraph applies to the Security Manager and not necessarily to the general Security Administration software.

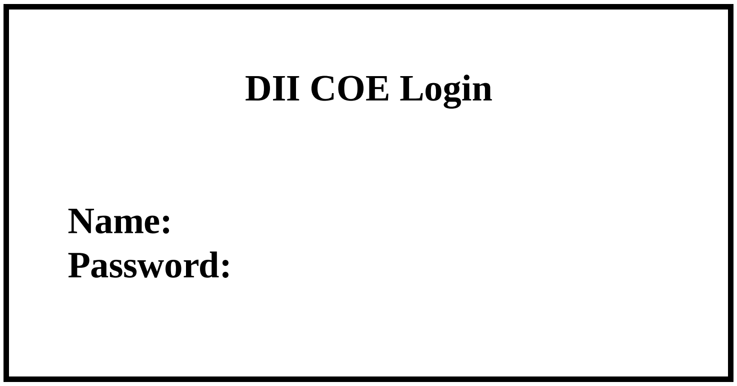
Access to Security Manager is specifically granted by the security administrator. Users who need to access Security Manager must be assigned to a profile that contains the Security Manager application. Only profiles that are derivatives of the `SSO_Default` account group can grant access to Security Manager.

4.1.6 Installation and Configuration

The Security Administration segment is packaged as a component of the DII COE Kernel and is therefore installed with the DII COE Kernel. For instructions on installing and configuring the DII COE Kernel containing the Security Administration software, see the *DII COE Installation Procedures for the Kernel Patch 2*. Prior to installation of Kernel Patch 2, installation of the DII COE Kernel Version 3.2.0.0 is required. For instructions on installing and configuring the DII COE Kernel Version 3.2.0.0, see the *DII COE Kernel Installation Guide*. DII COE Kernel Patch 2 does not require deinstallation of DII COE Kernel 3.2 Patch 1 prior to its installation.

4.2 Initiating a Session

To access DII COE Security Administration functionality, you must enter the `secman` login name and the `secman` password. Only user accounts assigned to profiles under the Security Admin account group may run Security Administration software. The `DII COE Login` screen (Figure 6) and the DISA security screen appear any time a machine loaded with the Solaris 2.5.1 Operating System and the DII COE Kernel is rebooted or any time a user logs out of the system at the console.



DII COE Login

Name:
Password:

Figure 6. DII COE Login Screen

To log in with a `secman` account and access DII COE Security Administration functionality, follow the steps below.

STEP 1: **Log in as the security administrator**. In the `DII COE Login` window (Figure 6), type `secman` in the `Name` field and press [RETURN].

STEP 2: **Enter the `secman` password**. In the `DII COE Login` window, type the `secman` password in the `Password` field and press [RETURN]. The Security Administration software appears.

STEP 3: **Access the Application Manager**. Double-click the `Application Manager` icon on the CDE panel. The `Application Manager` window appears. For additional information about CDE, see the *TriTeal Enterprise Desktop User's Guide*.

STEP 4: **Open the `DII_APPS` folder**. Double-click the `DII_APPS` folder. The `Application Manager - DII_APPS` window appears.

NOTE: Throughout this manual, it is assumed that you are modifying local accounts and profiles, as designated by options beginning with `L:`. To modify global accounts and profiles, use options beginning with `G:` instead.

STEP 5: **Open the `L:SSO_Default` folder**. Double-click the `L:SSO_Default` folder. The `Application Manager - L:SSO_Default` window appears.

The following paragraph applies to the Security Manager and not necessarily to the general Security Administration software.

Only those user accounts assigned to profiles under the `Security Admin` account group may run Security Manager. Double-click the `Security Manager` icon in the folder associated with an administrative profile in `Application Manager`; a window will appear similar to that shown in Figure 7, except it has a large empty body below.

Figure 7. EM Security Manager Main Window

If you experience problems while initiating a section, see the error recovery guidelines in the *DII COE System Administrator's Guide*.

4.3 Stopping and Suspending Work

Use of the Security Administration software segment is dependent upon assignment of applications to a profile and subsequent assignment of the profile to a user. The security administrator performs this assignment. Revocation of the profiles is only accomplished during the period when the user is not accessing that profiles.

To cease use of the DII COE Security Administration functionality, log out of the `secman` account. You have successfully logged out when the `DII COE Login` window appears (Figure 6).

To log out of the `secman` account, follow the steps below.

STEP 1: **Choose to logout of the account.** In the CDE Front Panel, click `EXIT`. The `Lougout Confirmation` window appears.

STEP 2: **Continue the logout**. Click `Continue logout`. The `DII COE Login` window appears.

The following paragraph applies to the Security Manager.

To quit using Security Manager, select `Exit` from the `File` menu. If you have made any changes that have not yet been committed, you will be prompted to either accept the transactions or discard them.

This page intentionally left blank.

5. DII COE Security Administration Processing Guide

NOTE: Throughout this manual, it is assumed that you are modifying local accounts and profiles, as designated by options beginning with L:. To modify global accounts and profiles, use options beginning with G: instead.

The Application Manager - L:SSO_Default window contains the following security management icons:

C Assign Passwords

C Audit Log File Manager

C Edit Profiles

C Profile Selector Config

C Security Manager

C Security Mgr Remote

C Unlock Users

C Update Security DB.

The Assign Passwords, Audit Log File Manager, Edit Profiles, Security Manager, and Unlock Users icons are described in the following subsections.

NOTE: Documentation for the Profile Selector Config, Security Mgr Remote, and Update Security DB icons and their associated functionality will be provided at a later date.

In addition to describing the icons above, this guide describes the Chg Password icon. To access this icon, select the DII_TOOLS folder from the Application Manager window. The Application Manager - DII_TOOLS window appears. The Application Manager - DII_TOOLS window contains the Chg Password icon.

5.1 Capabilities

The Security Administration segment provides the capability to establish, maintain and delete user accounts and UNIX groups and define profiles. In addition, the security administrator has the capability to manage the audit log files.

The Security Administrator account group serves as a template for establishing a runtime environment for the security administrator. It contains template files for specifying COE processes to launch at login time, functions to be made available to operators, and global default preferences such as color selections for window borders.

Once profiles have been created and defined, use the `Edit Profiles` icon to modify profiles to add and restrict access to functions that have menus and options.

The remainder of Section 5.1 applies to the Security Manager and not necessarily to the general Security Administration software.

The Security Manager interface design revolves around catalogs. There is one catalog for each of the four main types of objects you will need to modify: users, profiles, applications, and UNIX groups. Only one catalog can be active, or visible, at a time.

In general, begin Security Administration by activating the appropriate catalog and then interacting with the catalog using the functions provided with the three pull-down menus, or through interface short-cuts such as double-clicking an entry to modify it. For example, to add a new user, bring up the User Catalog and use the `New User` option under the `File` menu.

5.2 Conventions

User names or profiles may be either local or global. If both local and global objects are displayed on the same window, the object's name will be prefaced by either an `L:` or a `G:`, indicating that it is local or global respectively. For example, the profile name `G:SSO_Default` refers to the *global* `SSO_Default` profile, whereas the profile `L:Safe_Profile` refers to the safe profile defined on the *local* machine.

For a description of other conventions used by the software, see the *User Interface Specifications for the DII*.

5.3 Processing Procedures

The following sections provide instructions on using the System Administration capability of DII COE. The sections are arranged by the following functions:

C Assigning Passwords

C Modifying Profiles

C Unlocking Users

C Monitoring Hard Disk Capacity

C Managing the Audit Log Files

C Manually Deleting Audit Log Files

C Maintaining User Accounts

C Maintaining Profiles

C Viewing the Application Catalog

C Maintaining UNIX Groups

C Changing the secman Password.

Section 5.3.1, *Assigning Passwords*, must be completed before Section 5.3.2, *Modifying Profiles*, and Section 5.3.3, *Unlocking Users*.

The following procedure applies to the Security Manager.

The Security Manager provides a great deal of flexibility in setting up user accounts and profiles. However, you will find it easier if you perform these steps in the following order during your *initial* implementation of users and profiles:

STEP 1: **Load segments and generate the applications database**.

STEP 2: **Define profiles and assign applications to them**. Take time to consider how users are grouped and which applications you want which users to be able to access.

STEP 3: **Define any additional UNIX groups that your site will need**.

STEP 4: **Create new user accounts and add the users to the profiles and the UNIX groups you have previously defined**.

5.3.1 Assigning Passwords

Passwords can be changed for existing local or network user accounts using the `Assign Password` icon. Follow the steps below to assign passwords to existing user accounts.

STEP 1: **Log in as the security administrator**. In the `DII COE Login` window (Figure 6), type `secman` in the `Name` field and press [`RETURN`].

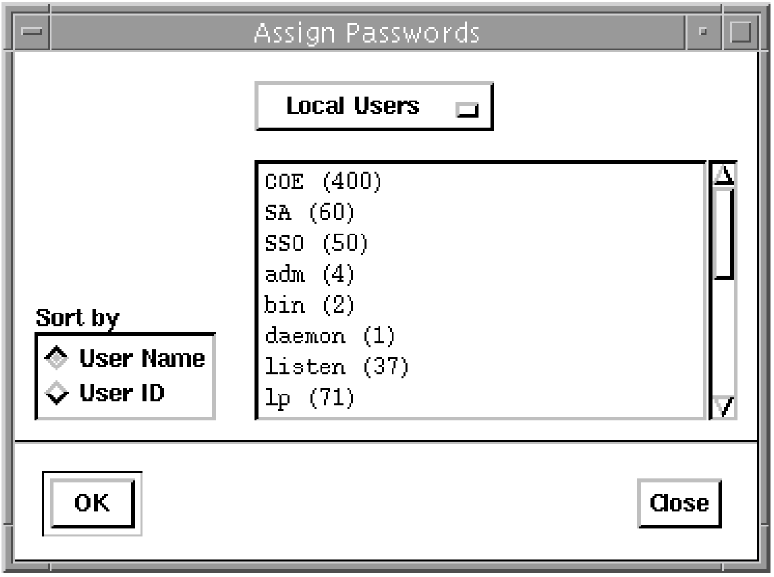
STEP 2: **Enter the `secman` password**. In the `DII COE Login` window, type the `secman` password in the `Password` field and press [`RETURN`]. The Security Administration software appears.

STEP 3: **Access the Application Manager**. Double-click the `Application Manager` icon on the CDE panel. The `Application Manager` window appears. For additional information about CDE, see the *TriTeal Enterprise Desktop User's Guide*.

STEP 4: **Open the `DII_APPS` folder**. Double-click the `DII_APPS` folder. The `Application Manager - DII_APPS` window appears.

STEP 5: **Open the `L:SSO_Default` folder**. Double-click the `L:SSO_Default` folder. The `Application Manager - L:SSO_Default` window appears.

STEP 6: **Select the `Assign Passwords` icon**. To open the `Assign Passwords` window (Figure 8), double-click the `Assign Passwords` icon. The window shown in Figure 8 contains a list of local user accounts sorted by user name because `User Name` is selected in the `Sort by` panel.



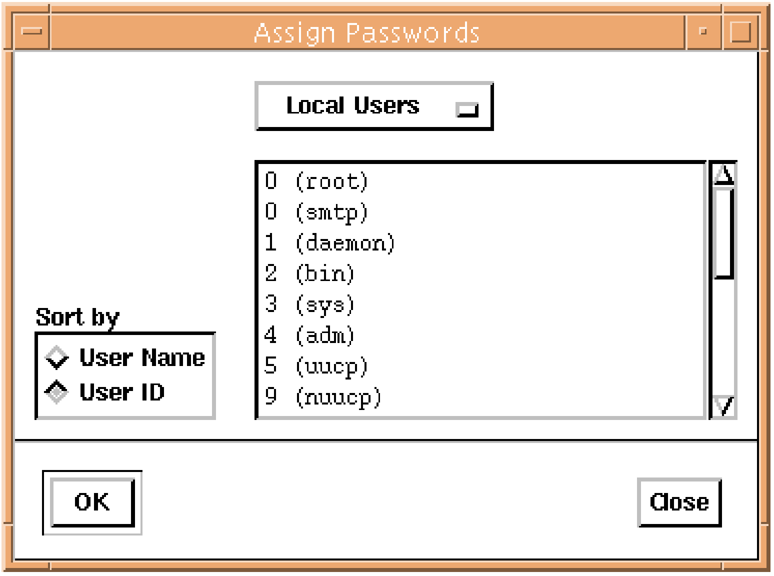
Local Users

Sort by
- ◆ User Name
- ◇ User ID

```
COE (400)
SA (60)
SSO (50)
adm (4)
bin (2)
daemon (1)
listen (37)
lp (71)
```

Figure 8. Assign Passwords Window (Sorted by User Name)

Figure 9 contains a list of local user accounts sorted by user ID because `User ID` is selected in the `Sort by` panel.



Local Users

Sort by
- ◇ User Name
- ◆ User ID

```
0 (root)
0 (smtp)
1 (daemon)
2 (bin)
3 (sys)
4 (adm)
5 (uucp)
9 (nuucp)
```

Figure 9. Assign Password Window (Sorted by User ID)

STEP 7: **Determine if you want to view a list of local user accounts or network user accounts**. To select either the `Local Users` option or the `Network Users` option, click the button at the top of the window.

STEP 8: **Determine if you want to view the list of user accounts by user name or by user ID**. In the `Sort by` panel, click either `User Name` or `User ID`.

STEP 9: **Select the user account for whom you want to assign a password**. Highlight a user account and click `OK`. The `Set Password` window appears (Figure 10).

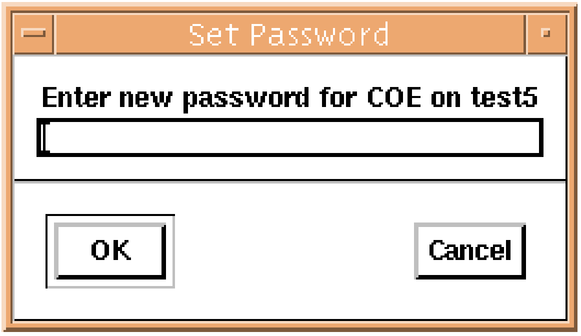


Figure 10. Set Password Window

STEP 10: **Enter a new password**. In the `Enter new password for [user name] on [machine name]` field, type a new password and click `OK`. The `Verify Password` window appears (Figure 11).

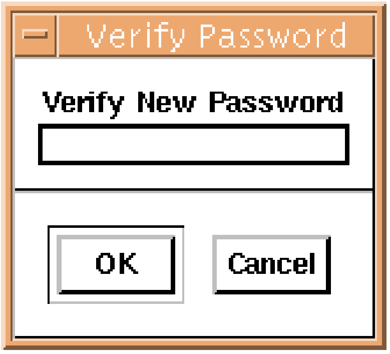


Figure 11. Verify Password Window

STEP 11: **Re-enter the password**. In the `Verify New Password` field, retype the password and click `OK`.

STEP 12: **Assign a password for other user accounts or exit the `Assign Password` window**. Assign a password for other user accounts by following STEPS 7-11 for each user account. When you are done assigning passwords to user accounts, click `Close` to exit the `Assign Password` window (Figure 8).

5.3.2 Modifying Profiles

Once created and defined, you can modify profiles to add and restrict access to functions within menus and options using the `Edit Profiles` icon. Follow the steps below to modify profiles.

STEP 1: **Log in as the security administrator**. In the `DII COE Login` window (Figure 6), type `secman` in the `Name` field and press [`RETURN`].

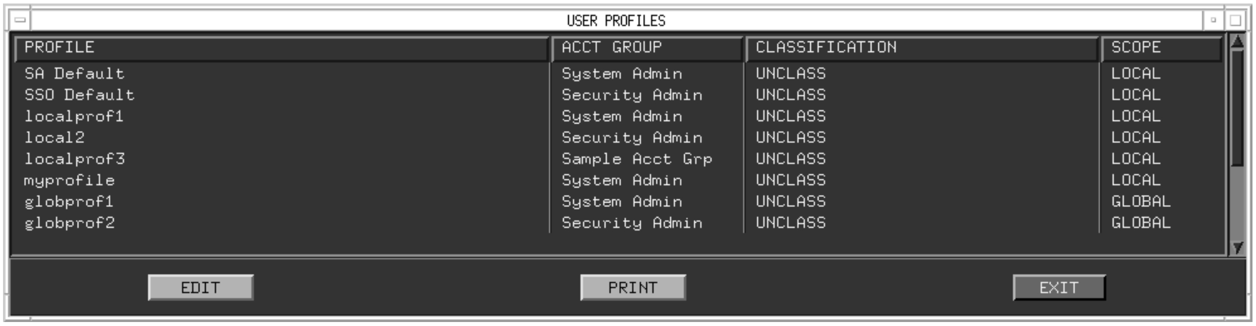
STEP 2: **Enter the `secman` password**. In the `DII COE Login` window, type the `secman` password in the `Password` field and press [`RETURN`]. The Security Administration software appears.

STEP 3: **Access the Application Manager**. Double-click the `Application Manager` icon on the CDE panel. The `Application Manager` window appears. For additional information about CDE, see the *TriTeal Enterprise Desktop User's Guide*.

STEP 4: **Open the `DII_APPS` folder**. Double-click the `DII_APPS` folder. The `Application Manager - DII_APPS` window appears.

STEP 5: **Open the `L:SSO_Default` folder**. Double-click the `L:SSO_Default` folder. The `Application Manager - L:SSO_Default` window appears.

STEP 6: **Select the `Edit Profiles` icon**. To open the `USER PROFILES` window (Figure 12), double-click the `Edit Profiles` icon. The `USER PROFILES` window lists all user profiles you can modify.



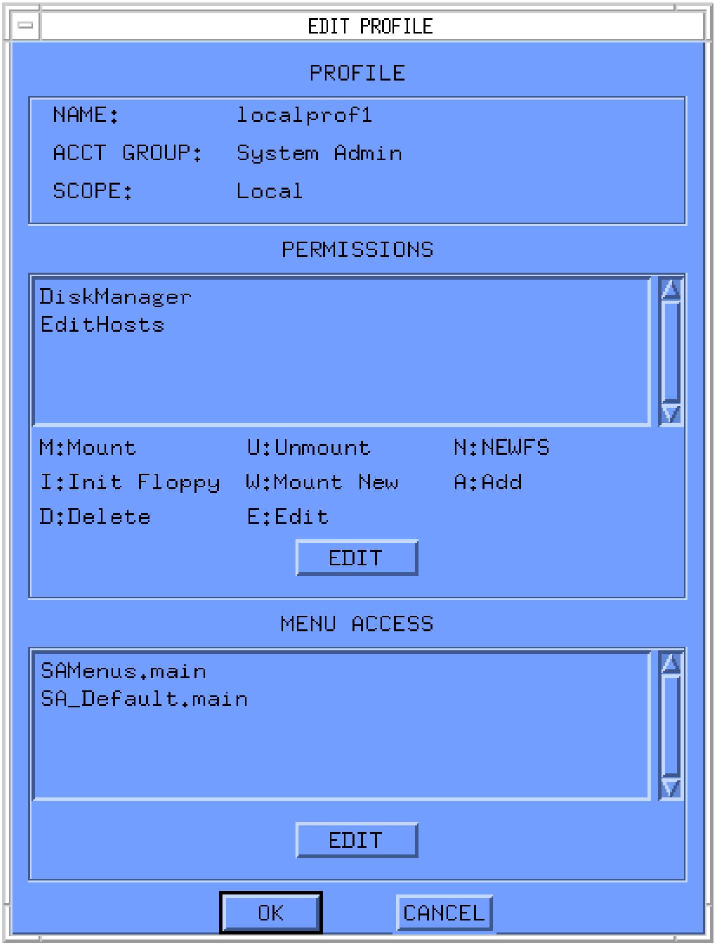
PROFILE	ACCT GROUP	CLASSIFICATION	SCOPE
SA Default	System Admin	UNCLASS	LOCAL
SSO Default	Security Admin	UNCLASS	LOCAL
localprof1	System Admin	UNCLASS	LOCAL
local2	Security Admin	UNCLASS	LOCAL
localprof3	Sample Acct Grp	UNCLASS	LOCAL
myprofile	System Admin	UNCLASS	LOCAL
globprof1	System Admin	UNCLASS	GLOBAL
globprof2	Security Admin	UNCLASS	GLOBAL

Figure 12. USER PROFILES Window

STEP 7: **Select a profile to modify**. To modify a profile’s access to functions within menus and options, select the profile and click `EDIT`.

NOTE: `SA Default` and `SSO Default` user profiles cannot be edited. If you select one of these, the `CANNOT MODIFY` warning window appears. To close it, click `OK`.

STEP 8: **Review the information in the `EDIT PROFILE` window**. The `EDIT PROFILE` window appears (Figure 13). The `PERMISSIONS` panel shows the applications that have been assigned to that profile.



EDIT PROFILE

PROFILE

NAME: localprof1

ACCT GROUP: System Admin

SCOPE: Local

PERMISSIONS

DiskManager
EditHosts

M:Mount U:Unmount N:NEWFS
I:Init Floppy W:Mount New A:Add
D:Delete E:Edit

MENU ACCESS

SAMenus.main
SA_Default.main

Figure 13. EDIT PROFILE Window

STEP 9: **Modify permissions, if desired**. To modify permission settings for an option, highlight the option in the `PERMISSIONS` panel and click `EDIT`. For example, in the `EDIT PROFILE` window (Figure 13), click a permission such as the `DiskManager` option and click `EDIT`.

STEP 10: **Set permissions for the option**. The `EDIT PERMISSIONS` window appears (Figure 14). Figure 14 shows `DISKMANAGER PERMISSIONS` because the `DiskManager` option was selected in STEP 8. Click the options for which the profile should have permissions. For example, if you want the profile to be able to mount a file system and unmount a file system, click `Mount` and `Unmount` in Figure 14. When you finish selecting options, click `OK`. The `EDIT PROFILE` window (Figure 13) returns to the forefront.

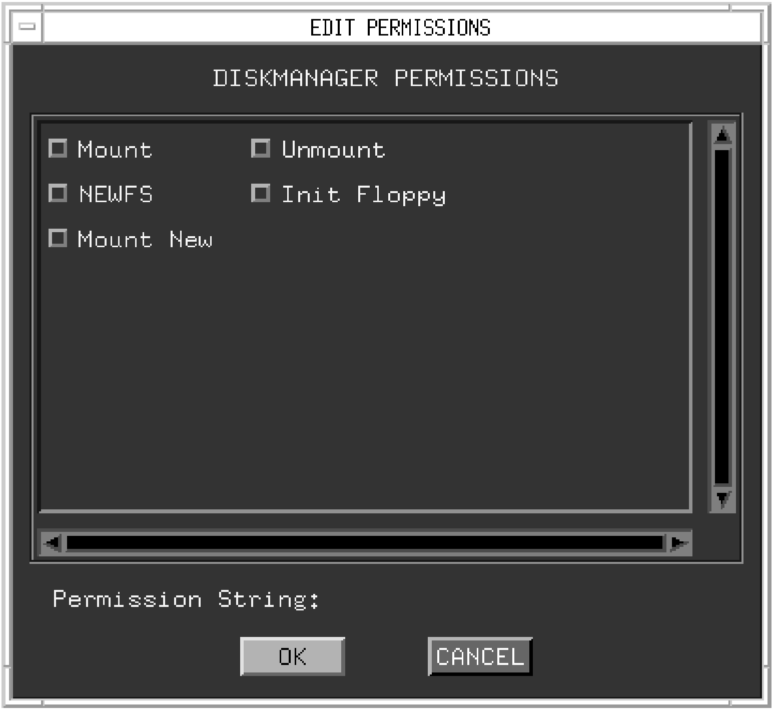


Figure 14. EDIT PERMISSIONS Window

STEP 11: **Modify menu access, if desired**. To modify menu access settings for the option, highlight a menu in the `MENU ACCESS` panel and click `EDIT`. For example, in the `EDIT PROFILE` window (Figure 13), click a menu access option such as the `SAMenus.main` option and click `EDIT`.

STEP 12: **Set menu access settings**. The `EDIT MENU ACCESS` window appears (Figure 15). Figure 15 shows System Administration menus because the `SAMenus.main` option was selected in STEP 10. Click the menus for which the profile should have permissions. For example, if you want the profile to have access to the `Help` menu and the `SA System` menu, click `Help` and `SA System` in Figure 15. When you finish selecting options, click `OK` . The `EDIT PROFILE` window (Figure 13) returns to the forefront.

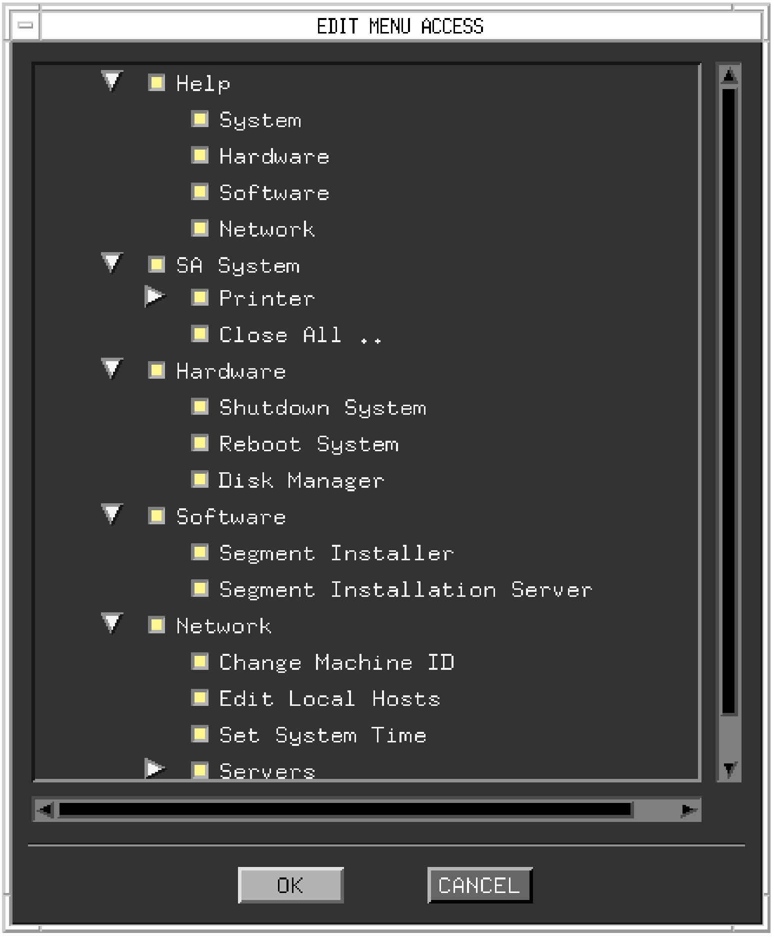


Figure 15. EDIT MENU ACCESS Window

STEP 13: **Apply your changes**. To apply your changes and exit the window, click `OK` in the `EDIT PROFILE` window (Figure 13).

5.3.3 Unlocking Users

A user account is disabled automatically the third consecutive time an incorrect password is entered for that account. When an account is disabled, a message similar to the following appears:

```
Account is disabled -- see Account Administrator.
```

Unlock disabled user accounts using the `Unlock Users` icon. Follow the steps below to re-enable a user account that has been disabled.

STEP 1: **Log in as the security administrator**. In the `DII COE Login` window (Figure 6), type `secman` in the `Name` field and press [RETURN].

STEP 2: **Enter the `secman` password**. In the `DII COE Login` window, type the `secman` password in the `Password` field and press [RETURN]. The Security Administration software appears.

STEP 3: **Access the Application Manager**. Double-click the `Application Manager` icon on the CDE panel. The `Application Manager` window appears. For additional information about CDE, see the *TriTeal Enterprise Desktop User's Guide*.

STEP 4: **Open the `DII_APPS` folder**. Double-click the `DII_APPS` folder. The `Application Manager - DII_APPS` window appears.

STEP 5: **Open the `L:SSO_Default` folder**. Double-click the `L:SSO_Default` folder. The `Application Manager - L:SSO_Default` window appears.

STEP 6: **Select the `Unlock Users` icon**. To open the `User Account Information` window (Figure 16), double-click the `Unlock Users` icon.

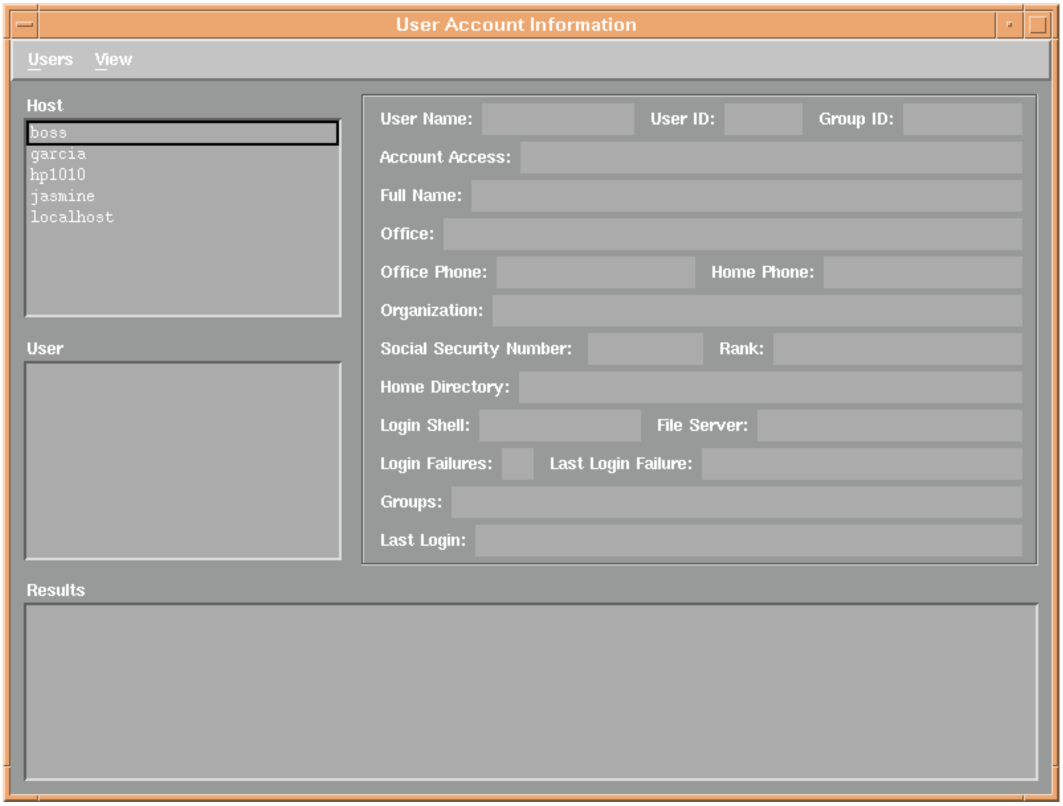


Figure 16. User Account Information Window

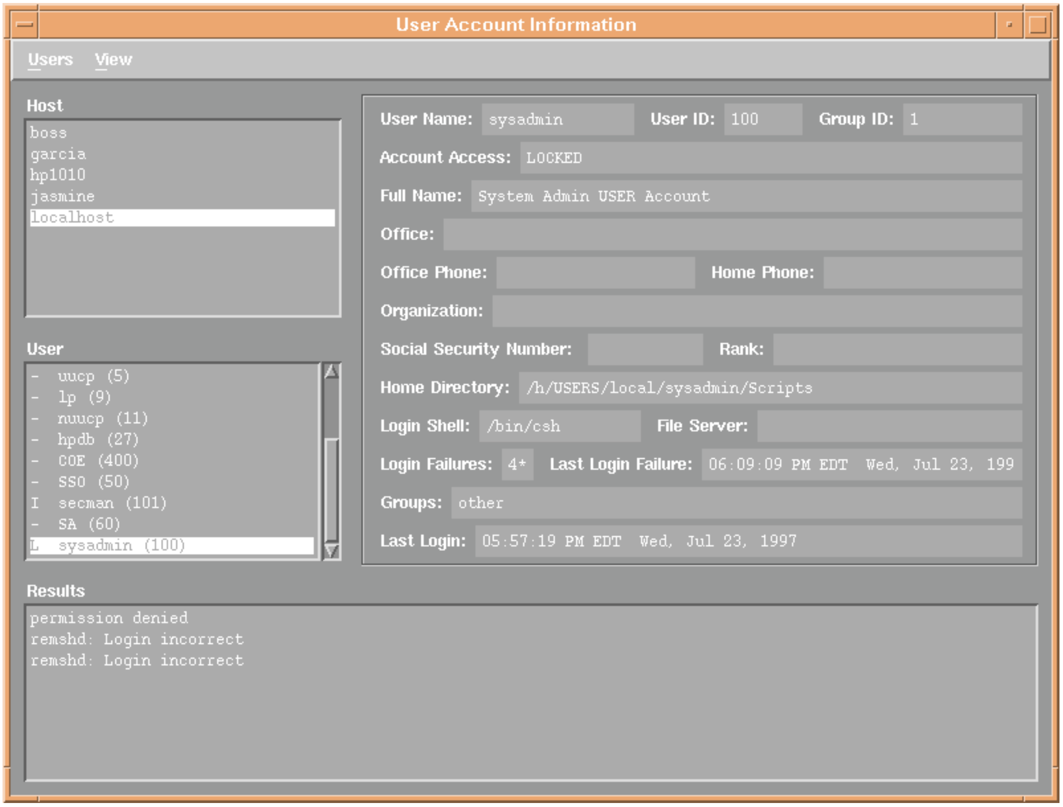
STEP 7: **Select the host machine for which a user has been locked out**. In the `Host` panel, click a host machine for which a user has been locked out. From the `Users` pull-down menu, select the `Update for Selected Host` option. *All* valid user accounts for the selected machine appear in the `User` panel by default.

NOTE: If you want to select the host machine you are currently using, select `localhost`.

STEP 8: **Determine if you want to view all user accounts or a subset of all user accounts**. If you want to view all user accounts, proceed to STEP 9. If you want to tailor the list of user accounts to view particular users, select the `Local Users` option, `Network Users` option, `Logged In Users` option, `Enabled Users` option, `Disabled Users` option, `Locked Out Users` option, or `Users with Failed Logins` option from the `View` pull-down menu. In the `User` panel, the letter `L` beside a user account indicates a locked account; the letter `F` beside a user account indicates an account with one or two login failures; and the letter `I` beside a user account name indicates the user account with which you logged in to the machine.

NOTE: If you just want to view a list of locked out users, select the `Locked Out Users` option. If you want to view a list of all user accounts with at least one login failure (including locked out users), select the `Users with Failed Logins` option.

STEP 9: **Select the user account that has been locked out of the selected host machine**. In the `User` panel, click a user account; the letter `L` should appear beside this user account. Information about that user account appears in the panel on the right side of the `User Account Information` window, as shown in Figure 17.



```
boss
garcia
hp1010
jasmine
localhost
```

```
-   uucp (5)
-   lp (9)
-   nuucp (11)
-   hpdb (27)
-   COE (400)
-   SSO (50)
I   secman (101)
-   SA (60)
L   sysadmin (100)
```

User Name: sysadmin User ID: 100 Group ID: 1
Account Access: LOCKED
Full Name: System Admin USER Account
Office:
Office Phone: Home Phone:
Organization:
Social Security Number: Rank:
Home Directory: /h/USERS/local/sysadmin/Scripts
Login Shell: /bin/csh File Server:
Login Failures: 4* Last Login Failure: 06:09:09 PM EDT Wed, Jul 23, 199
Groups: other
Last Login: 05:57:19 PM EDT Wed, Jul 23, 1997

```
permission denied
remshd: Login incorrect
remshd: Login incorrect
```

Figure 17. User Account Information Window with User Account Information

For example, in Figure 17, the `Account Access` field shows that the user account is `LOCKED`, the `Login Failures` field shows that more than three (4+) login failures have occurred, and the `Last Login Failure` field shows the date and time of the last login failure.

STEP 10: **Clear the selected user's login failures**. From the `Users` pull-down menu, select the `Clear Login Failures` option. In the `User` panel, the letter `L` no longer appears beside the cleared user account.

NOTE: If any commands do not work as expected, one or more messages appear in the `Results` panel of the window.

STEP 11: **Update information about the cleared user account**. To ensure that the user account is cleared, click the user account in the `User` panel. In the panel on the right side of the `User Account Information` window, the `Account Access` field updates to show that the user account is `ENABLED`.

STEP 12: **Exit the `User Account Information` window**. To exit the `User Account Information` window, select `Exit` from the `Users` pull-down menu.

5.3.4 Monitoring Hard Disk Capacity

The security administration software provides the ability to monitor the capacity of the hard disk. You may enable a check that notifies you of when the hard disk reaches a certain percentage of its full capacity. When you receive this warning, you may take the appropriate action to remove unnecessary files or save files to an external storage device. Activating hard disk monitoring will also activate audit log file monitoring. For additional information on monitoring the audit log files, see Section 5.3.5.1, *Monitoring the Audit Log Files*. Follow the steps below to monitor hard disk capacity.

STEP 1: **Log in as the security administrator**. In the `DII COE Login` window (Figure 6), type `secman` in the `Name` field and press [RETURN].

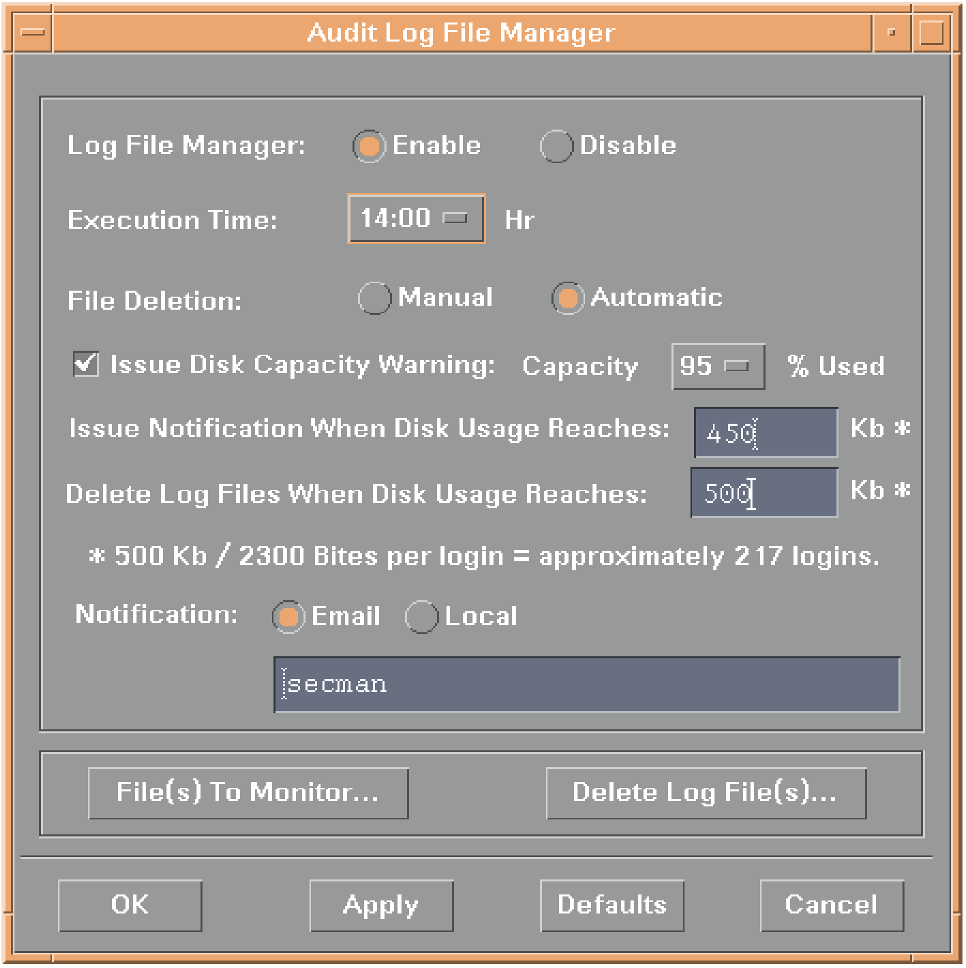
STEP 2: **Enter the `secman` password**. In the `DII COE Login` window, type the `secman` password in the `Password` field and press [RETURN]. The Security Administration software appears.

STEP 3: **Access the Application Manager**. Double-click the `Application Manager` icon on the CDE panel. The `Application Manager` window appears. For additional information about CDE, see the *TriTeal Enterprise Desktop User's Guide*.

STEP 4: **Open the `DII_APPS` folder**. Double-click the `DII_APPS` folder. The `Application Manager - DII_APPS` window appears.

STEP 5: **Open the `L:SSO_Default` folder**. Double-click the `L:SSO_Default` folder. The `Application Manager - L:SSO_Default` window appears.

STEP 6: **Open the `Audit Log File Manager` window**. Double-click the `Audit Log File Manager` icon. The `Audit Log File Manager` window appears (Figure 18).



Log File Manager: ● Enable ○ Disable

Execution Time: 14:00 Hr

File Deletion: ○ Manual ● Automatic

☑ Issue Disk Capacity Warning: Capacity 95 % Used

Issue Notification When Disk Usage Reaches: 450 Kb *

Delete Log Files When Disk Usage Reaches: 500 Kb *

* 500 Kb / 2300 Bites per login = approximately 217 logins.

Notification: ● Email ○ Local

secman

Figure 18. Audit Log File Manager Window

STEP 7: **Enable disk capacity monitoring**. In the `Log File Manager` field, click `Enable` to allow monitoring of the disk capacity.

STEP 8: **Choose the time for disk capacity monitoring**. The disk capacity will be monitored once a day. The default time is 14:00 Hr. To choose an hour for hard disk capacity monitoring, click the option button in the `Execution Time` field.

STEP 9: **Enable a disk capacity warning**. To get a warning once the hard disk reaches a certain percentage of its capacity, select `Issue Disk Capacity Warning.`

STEP 10: **Select the percentage of disk capacity**. To choose the percentage of the hard disk’s full capacity at which you want to receive a warning, click the option button in the `Capacity Used` field.

STEP 11: **Choose a method of notification**. In the Notification field, click Email to receive a message in your e-mail account or Local to have a warning appear on the screen that the disk is nearing its full capacity. If you choose Email, type your e-mail address in the data entry field. The address defaults to secman.

STEP 12: **Exit the Audit Log File Manager window**. To accept the disk capacity monitoring and exit the Audit Log File Manager window, click OK.

5.3.5 Managing the Audit Log Files

Whenever a user logs in using the DII COE Login Screen, an audit log file tracks the user's login. Over time, these login files could fill up, so the security administrator has the ability to manage the audit log files.

The Solaris audit log consists of the following files: wtmp, wtmpx, utmp, and utmpx. These files hold user and accounting information for commands such as who, write, and login.

Whenever the audit log files are deleted, an entry is made in the syslog.log file located in the var/adm/syslog directory.

The following two sections provide instructions for monitoring the audit log files and for manually deleting audit log files.

5.3.5.1 Monitoring the Audit Log Files

During installation of the DII COE Kernel, the user may choose to enable monitoring of the audit log files. For more information about enabling audit log file monitoring during installation, see the *DII COE Installation Procedures for the Kernel*. Once the Kernel has been installed, follow the steps below to monitor the audit log files.

STEP 1: **Log in as the security administrator**. In the DII COE Login window (Figure 6), type secman in the Name field and press [RETURN].

STEP 2: **Enter the secman password**. In the DII COE Login window, type the secman password in the Password field and press [RETURN]. The Security Administration software appears.

STEP 3: **Access the Application Manager**. Double-click the Application Manager icon on the CDE panel. The Application Manager window appears. For additional information about CDE, see the *TriTeal Enterprise Desktop User's Guide*.

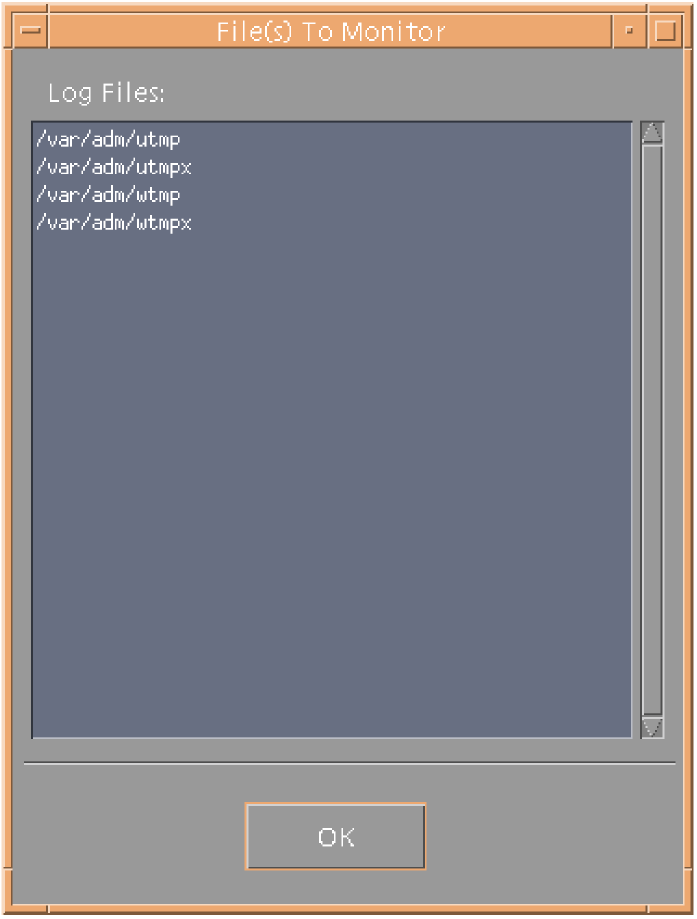
STEP 4: **Open the DII_APPS folder**. Double-click the DII_APPS folder. The Application Manager - DII_APPS window appears.

STEP 5: **Open the `L:SSO_Default` folder**. Double-click the `L:SSO_Default` folder. The `Application Manager - L:SSO_Default` window appears.

STEP 6: **Open the `Audit Log File Manager` window**. To open the `Audit Log File Manager` window (Figure 18), double-click the `Audit Log File Manager` icon.

STEP 7: **Choose to enable or disable log file monitoring**. In the `Log File Manager` field, click `Enable` to allow monitoring of the log file capacity.

STEP 8: **View the files to monitor**. To open the `File(s) to Monitor` window (Figure 19), click `File(s) to Monitor`. The window lists the system's audit log files that will be monitored. To close the window, click `OK`.



/var/adm/utmp
/var/adm/utmpx
/var/adm/wtmp
/var/adm/wtmpx

Figure 19. File(s) to Monitor Window

STEP 9: **Choose the time for log file monitoring**. The audit log will be monitored once a day. The default time is 14:00 hr. To choose an hour for log file monitoring, click the option button in the `Execution Time` field.

STEP 10: **Choose a method for log file deletion**. When a log file becomes too full, you may have the system automatically delete the file or you may manually delete it. The system default is manual deletion. In the `File Deletion` field, click `Manual` to delete the files yourself or `Automatic` to allow the system to delete the files. For instructions on manually deleting audit log files, see Section 5.3.5.2, *Manually Deleting Audit Log Files*. When a user logs in again after a file has been deleted, the system will regenerate the appropriate audit log file.

NOTE: The minimum file size for notification or deletion is 10K. The maximum size is 20,000K.

STEP 11: **Choose the size of the audit log at which a warning message is issued**. In the `Issue Notification When Disk Usage Reaches` field, enter the size of the log files in kilobytes at which you want to receive a warning. If you are using manual deletion, go to Step 13.

NOTE: To receive a warning message before the audit log files are deleted, select a larger size in the `Delete Log Files When Disk Usage Reaches` field than in the `Issue Notification When Disk Usage Reaches` field. When you receive the warning, you can then choose to back up the log audit files on another storage device before the files are automatically deleted.

STEP 12: **Choose the size of the audit log at which the files will be deleted**. In the `Delete Log Files When Disk Usage Reaches` field, enter the size of the log file disk in kilobytes at which you want the disk to be deleted.

STEP 13: **Choose a method of notification**. In the `Notification` field, click `Email` to receive a message in your e-mail account or `Local` to have a warning appear on the screen that the audit log files have reached the size you set in the `Issue Notification When Disk Usage Reaches` field. If you choose `Email`, type your e-mail address in the data entry field. The address defaults to `secman`.

STEP 14: **Exit the `Audit Log File Manager` window**. To accept the audit log file monitoring and exit the `Audit Log File Manager` window, click `OK`.

5.3.5.2 Manually Deleting Audit Log Files

When you receive a warning that the audit log files have reached their specified limit and you have not set your system for automatic deletion, you should manually delete the audit log files. For additional information on monitoring the size of the audit log files and automatic deletion, see Section 5.3.5.1, *Monitoring the Audit Log Files*. Follow the steps below to manually delete audit log files.

STEP 1: **Log in as the security administrator**. In the `DII COE Login` window (Figure 6), type `secman` in the `Name` field and press [`RETURN`].

STEP 2: **Enter the `secman` password**. In the `DII COE Login` window, type the `secman` password in the `Password` field and press [`RETURN`]. The Security Administration software appears.

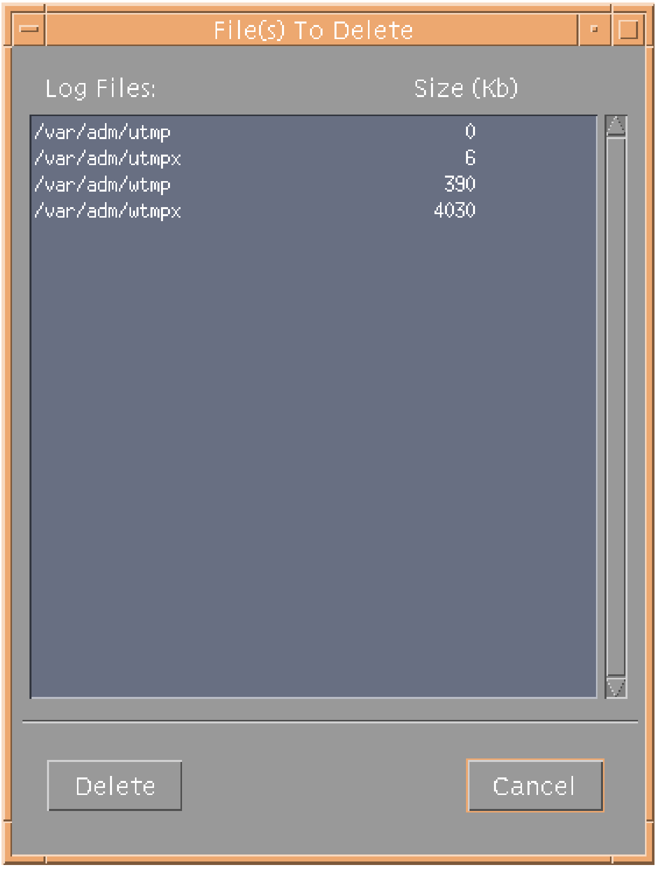
STEP 3: **Access the Application Manager**. Double-click the `Application Manager` icon on the CDE panel. The `Application Manager` window appears. For additional information about CDE, see the *TriTeal Enterprise Desktop User's Guide*.

STEP 4: **Open the `DII_APPS` folder**. Double-click the `DII_APPS` folder. The `Application Manager - DII_APPS` window appears.

STEP 5: **Open the `L:SSO_Default` folder**. Double-click the `L:SSO_Default` folder. The `Application Manager - L:SSO_Default` window appears.

STEP 6: **Open the `Audit Log File Manager` window**. Double-click the `Audit Log File Manager` icon. The `Audit Log File Manager` window appears (Figure 18).

STEP 7: **View the list of files you are going to delete**. To open the `File(s) to Delete` window (Figure 20), click `Delete Log File(s)`. The window lists the files you are about to delete and their size in kilobytes.



```
Log Files:                     Size (Kb)
/var/adm/utmp                  0
/var/adm/utmpx                 6
/var/adm/wtmp                  390
/var/adm/wtmpx                 4030
```

Figure 20. File(s) to Delete Window

STEP 8: **Delete the files**. To delete the audit log files and return to the `Audit Log File Manager` window (Figure 18), click `Delete`.

STEP 9: **Verify deletion of the files**. To open the `File(s) to Delete` window (Figure 20), click `Delete Log File(s)` again. Verify that the size of each file is correct and click `Cancel` to return to the `Audit Log File Manager` window (Figure 18).

STEP 10: **Exit the `Audit Log File Manager` window**. To exit the `Audit Log File Manager` window, click `OK` .

5.3.6 Maintaining User Accounts

The User Catalog provides tools to administer both local and global user accounts. Unlike previous versions of Security Manager, this interface now allows the Security Manager to create the user, assign them to additional UNIX groups, and assign them to profiles all from a single screen. Follow the steps below to access the User Catalog.

STEP 1: **Log in as the security administrator**. In the `DII COE Login` window (Figure 6), type `secman` in the `Name` field and press [`RETURN`].

STEP 2: **Enter the `secman` password**. In the `DII COE Login` window, type the `secman` password in the `Password` field and press [`RETURN`]. The Security Administration software appears.

STEP 3: **Access the Application Manager**. Double-click the `Application Manager` icon on the CDE panel. The `Application Manager` window appears. For additional information about CDE, see the *TriTeal Enterprise Desktop User's Guide*.

STEP 4: **Open the `DII_APPS` folder**. Double-click the `DII_APPS` folder. The `Application Manager - DII_APPS` window appears.

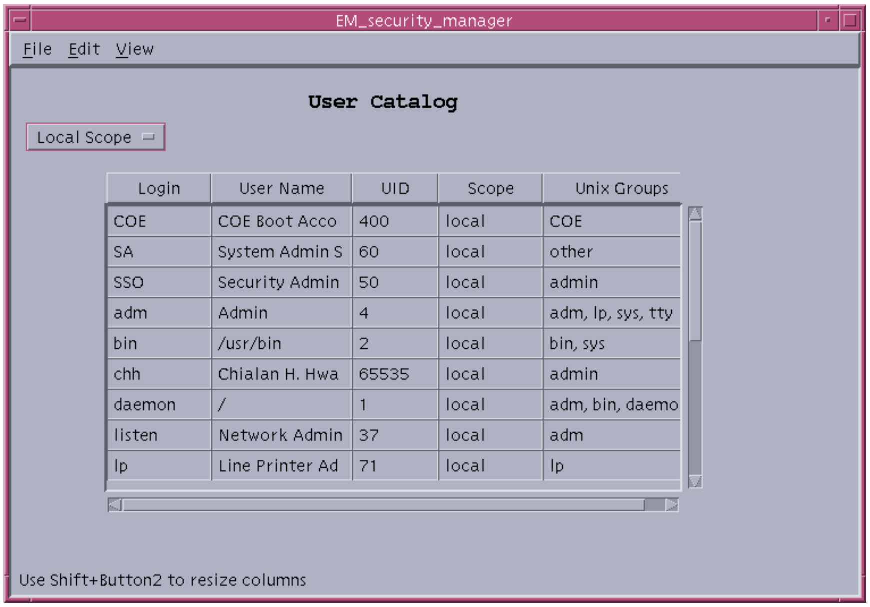
STEP 5: **Open the `L:SSO_Default` folder**. Double-click the `L:SSO_Default` folder. The `Application Manager - L:SSO_Default` window appears.

STEP 6: **Open the Security Manager**. To open the Security Manager, double-click the `Security Manager` icon.

STEP 7: **Display the User Catalog**. From the `View` pull-down menu, select `Users`. The User Catalog appears.

5.3.6.1 User Catalog

The User Catalog provides an overview of the user accounts that have been defined in the selected scope (i.e., local, global, or both). To display the User Catalog, choose `Users` from under the `View` pull-down menu. A display, similar to that shown in Figure 21, will appear.



User Catalog

Login	User Name	UID	Scope	Unix Groups
COE	COE Boot Acco	400	local	COE
SA	System Admin S	60	local	other
SSO	Security Admin	50	local	admin
adm	Admin	4	local	adm, lp, sys, tty
bin	/usr/bin	2	local	bin, sys
chh	Chialan H. Hwa	65535	local	admin
daemon	/	1	local	adm, bin, daemo
listen	Network Admin	37	local	adm
lp	Line Printer Ad	71	local	lp

Use Shift+Button2 to resize columns

Figure 21. User Catalog

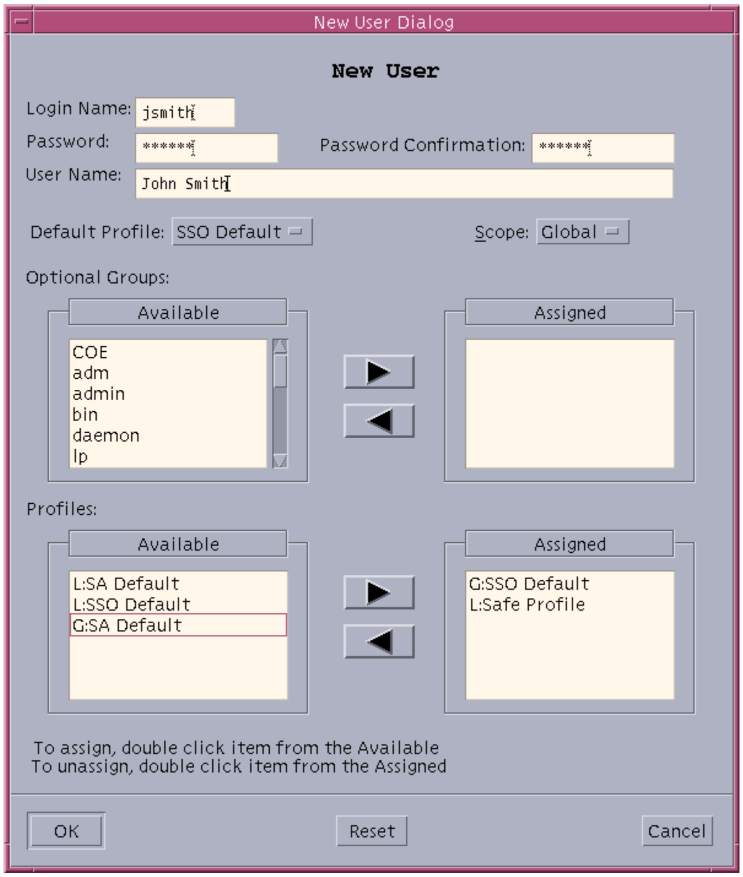
The catalog provides a summary of the accounts available and enough information for you to quickly identify the entry of interest. Additional detailed information about the users, such as the profiles which they have, are available by double-clicking on the individual entries to bring up the modify user window.

The User Catalog contains the following fields:

Field Name	**Description**
`Login`	User's login name.
`User Name`	The user's full name.
`UID`	The ID number assigned to this user by Security Manager and stored in the `/etc/passwd` or NIS password entry.
`Scope`	The account's scope. Currently either local or global.
`UNIX Groups`	A listing of the UNIX groups to which the user belongs. This will also include the user's default UNIX group.

5.3.6.2 Creating Accounts

To create a user account, activate the User Catalog by selecting `Users` from under the `View` menu. Next, select `New User` from under the `File` menu. A data entry screen appears, similar to the one shown in Figure 22. If the `New User` option is disabled in the `File` menu, Security Manager has been configured to *not* manage user accounts (refer to the `modify_accounts` token in the Security Manager configuration file described in Section 4.1.3 for more details.)



Login Name: jsmith
Password: ******
Password Confirmation: ******
User Name: John Smith
Default Profile: SSO Default
Scope: Global

Optional Groups: Available: COE, adm, admin, bin, daemon, lp

Profiles: Available: L:SA Default, L:SSO Default, G:SA Default
Assigned: G:SSO Default, L:Safe Profile

To assign, double click item from the Available
To unassign, double click item from the Assigned

Figure 22. New User Dialog Window

The `Create Account` window contains the following fields:

`Login Name`

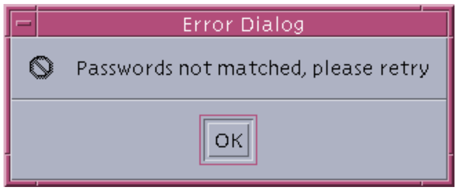
8-character alphanumeric field for the user login name. Login names must be distinct across scopes. You *may not* have a local and global account with the same login name. If you enter a login name that is either too short or too long, an error dialog box appears and you need to correct the entry before you continue.

`Password`

10-character field for the account's login password. Typed text is not shown in the field.

`Password Confirm`

10-character field for the Administrator to reenter the password. Because the typed text is not shown in the `Password` field, reenter the password to confirm that you typed it correctly. If the password in this field does not match that in the original `Password` field, an error dialog box, similar to that shown in Figure 23, will appear. Before proceeding further, edit one or both of the `Password` boxes.



Passwords not matched, please retry

Figure 23. Password Mismatch Dialog

`User Name`

40-character field for the name of the account holder, or any additional information that you want to maintain in this field.

`Default Profile`

Default profile for the account. This field initially displays the default profile defined in the Security Manager configuration file for the current scope. All profiles defined for the scope are listed in the popup list. Selecting a profile from the popup list will load it into the `Default Profile` field.

NOTE: Assigning the user to a default profile also assigns the user's default GID to the UNIX group associated with the default profile's parent account group.

`Scope`

Scope of the user's account. The popup contains a list of available scopes, currently defined as either `Local` or `Global`.

`Optional Groups`

The `Available` window on the left contains a scrolled list of any optional UNIX groups that can be assigned to the user that are currently not assigned to the user. By definition, the scope of a UNIX group must be identical to the user's scope (e.g., a local user can only be assigned to local groups). To assign a group to the user, click the name of the group in the left window and click the right arrow button >. The selected UNIX group moves from the `Available` panel to the `Assigned` panel. Alternately, double-click a UNIX group in the `Available` panel to transfer it to the `Assigned` panel. To unassign a group from a user, select the UNIX group in the `Assigned` panel and click the left arrow button <. Alternately, double-click an entry in the `Assigned` list to transfer it to the `Available` list. All optional groups assigned to an account as well as the group associated with the user's default profile appear under the `UNIX Groups` listing on the User Catalog.

Profiles

The Available panel contains a scrolled list of profiles that have been defined by the security administrator for the scope selected and that have not already been assigned to the user. The Assigned panel contains a listing of the profiles that have been assigned to the user. To assign a profile to the user, click the profile name in the Available panel and click the right arrow >. The profile transfers from the Available to the Assigned panel. Alternately, double-click the profile name in the Available panel and it transfers to the Assigned panel. To remove a profile assigned to a user, click the profile name in the Assigned panel and click the left arrow button <. The profile moves from the Assigned to the Available window. Alternately, double-click the profile in the Assigned panel to move the entry from the Assigned panel to the Available panel.

You *must* provide entries for all fields in the New User Dialog; only the Assigned field in the Optional Groups section may be left blank.

If you have completed entering the user data, select OK to submit the new user's information, Reset to change the display back to its original form, or Cancel to return to the Catalog without making any changes.

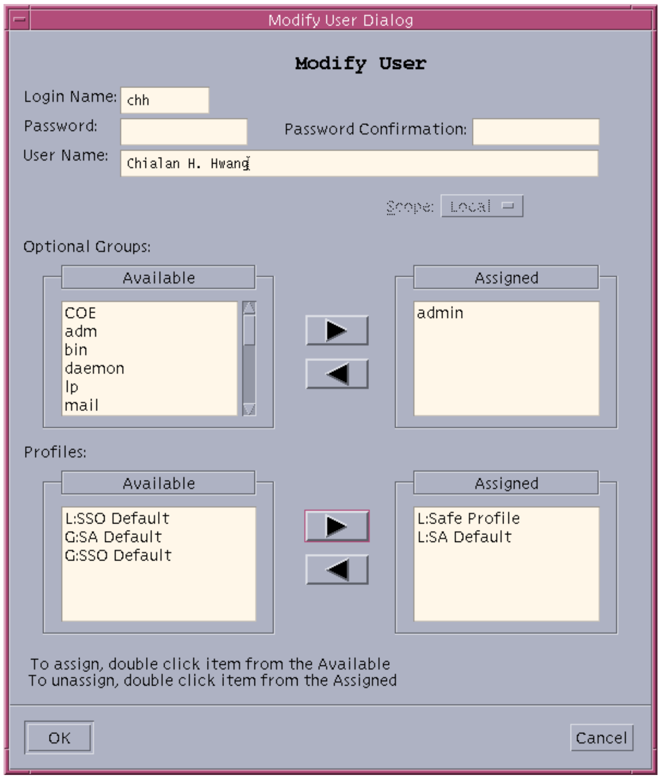
Once you click OK, Security Manager begins processing your request and may respond with one or more error messages. For example, if you try to create a new user using a login name already in use, an error dialog indicates that a duplicate user name has been detected. Dismiss the error dialog box and edit the Login Name field of the New User Dialog and click OK to resubmit your request to add a new user.

Once the account has been successfully created, Security Manager returns to the User Catalog, which will now contain the new user entry. If for some reason the new user's entry does not appear, click one of the headings to refresh the display.

5.3.6.3 Modifying an Account

Security Manager allows you to modify much of the data associated with a user after the user has been created. For example, you can change the user name, password, UNIX groups of which they are a member, and their assigned profiles. However, you may *not* change the user's login name or the scope of their account.

To modify a user's entry, bring up the User Catalog by selecting Users from the View menu. Double-click the entry you wish to change. You may need to use the scroll bars to move through the list to find the appropriate entry. This will bring up the Modify User Dialog window similar to the one shown in Figure 24.



Login Name: chh
Password:
Password Confirmation:
User Name: Chialan H. Hwang
Scope: Local

Optional Groups:

Available	Assigned
COE adm bin daemon lp mail	admin

Profiles:

Available	Assigned
L:SSO Default G:SA Default G:SSO Default	L:Safe Profile L:SA Default

To assign, double click item from the Available
To unassign, double click item from the Assigned

Figure 24. Modify User Dialog Window

The `Modify User Dialog` behaves identically to the `Create User Dialog`. To change the password, type the new password in both the `Password` and `Password Confirmation` boxes.

NOTE: The Change Password tool provided as part of the DII COE Kernel should be used to change passwords rather than this interface since the Change Password tool performs a much more rigorous check of the password entered.

Assign or unassign the user to or from UNIX groups and to or from profiles by moving entries between the `Available` and `Assigned` lists. To move an entry, either select it once and choose the appropriate arrow button (> to move from `Available` to `Assigned` or < to move from `Assigned` to `Available`). You can also double-click an entry to automatically transfer it from one list to the other.

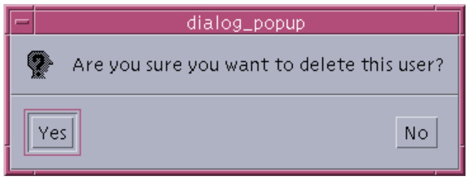
Once you have completed making your changes, click `OK` to begin processing the changes, or `Cancel` to discard the changes you have made. Either option will return you to the previous Catalog.

NOTE: A user must have a profile. If you remove all of the profiles from a user, a dialog box indicated that your entry has invalid input will be displayed. Add the user to a profile and then click OK or click Cancel to abandon your changes.

5.3.6.4 Deleting an Account

Security Manager provides the ability to delete user accounts. Deleting an account will result in removing all of the entries for the user in the user-profile database as well as deleting the user's home directory. Make sure you really want to delete the user's account before you proceed. If you need to temporarily remove the user's access to the system, you might want to enter a new password for the user.

To delete a user, first bring up the User Catalog by choosing Users from under the View menu. Highlight the entry you want to delete from the Catalog. You may need to use the scroll bars. To delete the entry, select Delete User from the Edit menu. A dialog box appears, similar to the one shown in Figure 25. To delete the user, click Yes; to cancel the delete operation, click No.



dialog_popup

Are you sure you want to delete this user?

Figure 25. Delete Account Dialog

NOTE: If you want to preserve the account directory and files, move them to a safe location out of the /h/USERS structure. If another account is created with the same login name and scope, it will overwrite the existing directory with a blank user account directory structure.

5.3.7 Maintaining Profiles

Security Manager maintains the user-profile database. Profiles are used to provide users with easy access to data and applications based on their functional needs. Additional detailed information about the profile, such as the applications which are currently assigned to it, is available by double-clicking on the individual entries to bring up the Modify User Dialog window (Figure 26). Follow the steps below to access the Profile Catalog.

STEP 1: **Log in as the security administrator**. In the DII COE Login window (Figure 6), type secman in the Name field and press [RETURN].

STEP 2: **Enter the secman password**. In the DII COE Login window, type the secman password in the Password field and press [RETURN]. The Security Administration software appears.

STEP 3: **Access the Application Manager**. Double-click the `Application Manager` icon on the CDE panel. The `Application Manager` window appears. For additional information about CDE, see the *TriTeal Enterprise Desktop User's Guide*.

STEP 4: **Open the `DII_APPS` folder**. Double-click the `DII_APPS` folder. The `Application Manager - DII_APPS` window appears.

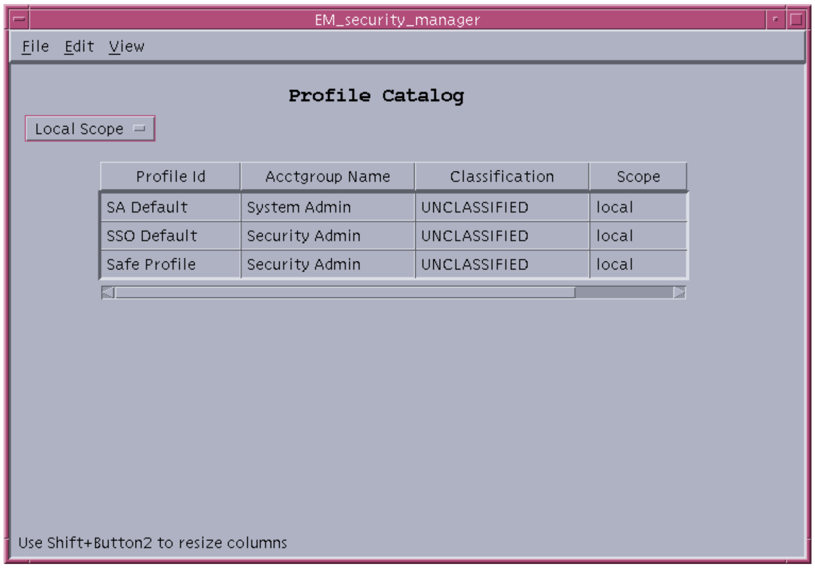
STEP 5: **Open the `L:SSO_Default` folder**. Double-click the `L:SSO_Default` folder. The `Application Manager - L:SSO_Default` window appears.

STEP 6: **Open the Security Manager**. To open the Security Manager, double-click the `Security Manager` icon.

STEP 7: **Display the Profile Catalog**. From the `View` pull-down menu, select `Profiles`. The Profile Catalog appears.

5.3.7.1 Profile Catalog

The `Profile Catalog` provides a listing of the profiles defined in the selected scope (i.e., local, global, or both), the account group to which they belong, and the profile's scope. To display the `Profile Catalog`, choose `Profile Catalog` from under the `View` pull-down menu. A display, similar to that shown in Figure 26, will appear.



Profile Catalog

Profile Id	Acctgroup Name	Classification	Scope
SA Default	System Admin	UNCLASSIFIED	local
SSO Default	Security Admin	UNCLASSIFIED	local
Safe Profile	Security Admin	UNCLASSIFIED	local

Use Shift+Button2 to resize columns

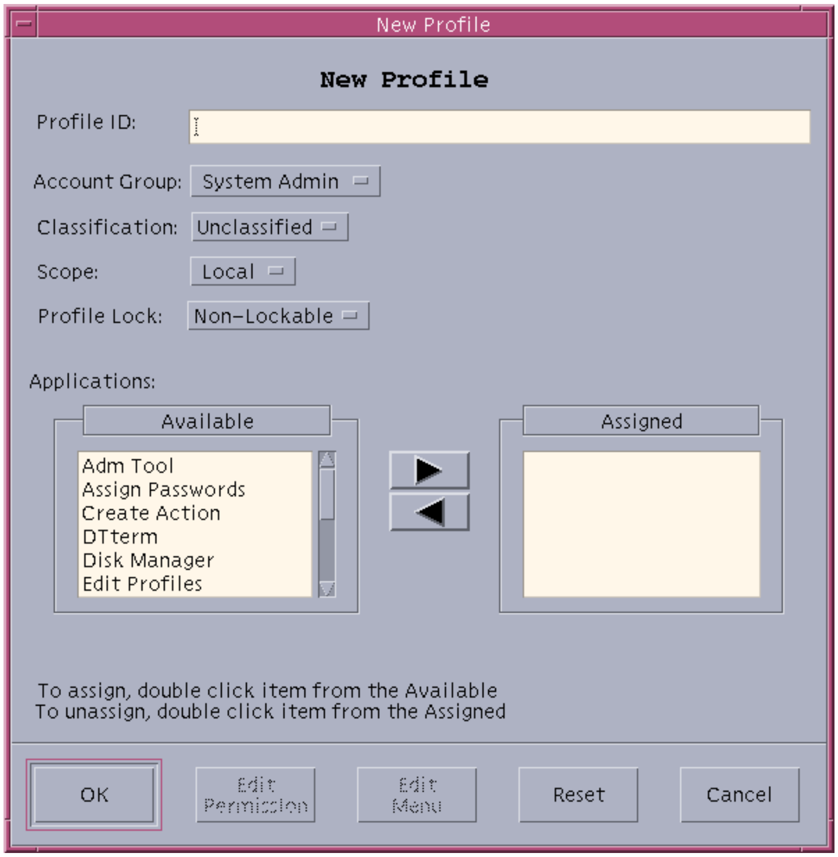
Figure 26. Profile Catalog

The Profile Catalog contains the following fields:

Field Name	Description
`Profile Name`	The name of the profile. This must be unique within the scope. It may be up to 50 characters in length.
`Account Group`	The name of the account group to which this profile belongs.
`Classification`	The classification level of the profile. Note that this currently has no impact on actual processing, nor should it be implied to provide any support for multi-level security.
`Scope`	The scope of the profile. Currently this is either `local` or `global`.

5.3.7.2 Creating Profiles

To create a new profile, activate the `Profile Catalog` by selecting `Profiles` from the `View` menu. Next, select `New Profile` from the `File` menu. A data entry screen, similar to the one shown in Figure 27, will appear.



New Profile

Profile ID:

Account Group: System Admin

Classification: Unclassified

Scope: Local

Profile Lock: Non-Lockable

Applications:

Available:

Adm Tool
Assign Passwords
Create Action
DTterm
Disk Manager
Edit Profiles

Assigned:

To assign, double click item from the Available
To unassign, double click item from the Assigned

Figure 27. New Profile Window

Enter the following information into the fields provided:

`Profile ID`

Enter the alphanumeric name of the profile. The profile's name must be unique within the scope. The only profile name which has any special impact on system behavior is the profile with the name `Safe Profile`.

`Account Group`

Select the account group to which this profile will belong. The account group determines the maximum set of application icons which can be assigned to the profile. In effect, a profile implements a subset of the icons that are part of a single account group.

`Classification`

Select the classification level from the pull-down list. This field is currently for informational purposes only and has no impact on the behavior of the system.

`Scope`

Use the pull-down list to set the scope of the profile. Currently, this scope is either local or global. If you are making a safe profile, you should consider making the profile a *local* profile.

`Profile Lock`

Use the pull-down list to define whether the profile can be `Lockable` or `Non-Lockable`. If you are creating a safe profile, be sure to make it `Non-Lockable`.

`Applications`

The `Available` panel contains a scrolled list of application icons that are part of the specified account group and that have not already been assigned to the profile. The `Assigned` panel contains a listing of the application icons assigned to the profile. To assign an application to the profile, click the application name in the `Available` window and click the right arrow `>`. The application transfers from the `Available` to the `Assigned` panel. Alternately, double-click application name in the `Available` panel and it transfers to the `Assigned` panel. To remove an application assigned to a profile, click the application name in the `Assigned` panel and click the left arrow button `<`. The application moves from the `Assigned` to the `Available` panel. Alternately, double-click the application name in the `Assigned` panel to move the entry from the `Assigned` to the `Available` panel.

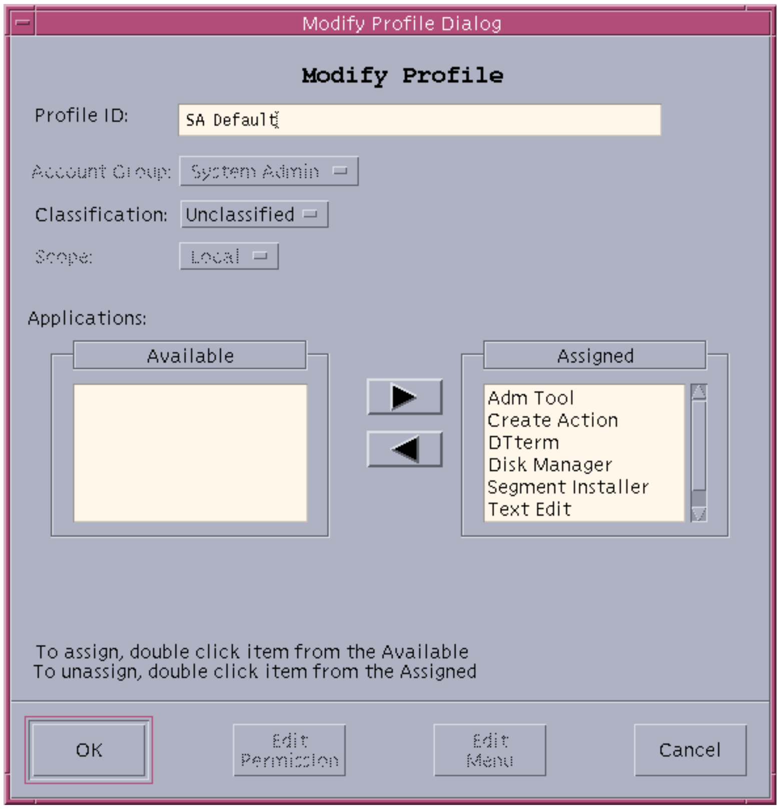
Once you have completed your entry, click `OK` to instruct the system to add your new profile, `Reset` to clear all of the changes you made to the dialog, or `Cancel` to discard your changes and return to the Profile Catalog.

The `Edit Permission` and `Edit Menu` buttons are grayed out, indicating that the functionality is not yet incorporated into Security Manager. If you need these services, execute the `Edit Permissions` icon directly.

5.3.7.3 Modifying Profiles

Security Manager allows you to modify much of the data associated with a profile after it has been created. For example, you can change the profile name, its classification level, and the list of applications assigned to the profile. However, you may *not* change the profile's account group or its scope.

To modify a profile's entry, bring up the Profile Catalog by selecting `Profiles` from the `View` menu. Double-click the entry you want to change. You may need to use the scroll bars to move through the list to find the appropriate entry. The `Modify Profile Dialog` window appears, similar to the one shown in Figure 28.



Modify Profile

Profile ID: SA Default

Account Group: System Admin

Classification: Unclassified

Scope: Local

Applications:

Available

Assigned

Adm Tool
Create Action
DTterm
Disk Manager
Segment Installer
Text Edit

To assign, double click item from the Available
To unassign, double click item from the Assigned

Figure 28. Modify Profile Dialog Window

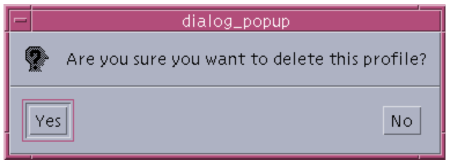
Change the profile's name by directly editing the `Profile ID` box. Update the classification by using the pull-down list to select a new classification level. Assign or unassign application icons to or from the profile by moving entries between the `Available` and `Assigned` lists. To move an entry, select it once and choose the appropriate arrow button (> to move from `Available` to `Assigned` or < to move from `Assigned` to `Available`). You can also double-click an entry to transfer it from one list to the other.

Once you have completed making your changes, click OK to begin processing the changes or Cancel to discard the changes you have made. Either option will return you to the previous Catalog. The Edit Permissions and Edit Menu buttons are inactive and will remain so until the next Security Manager upgrade.

5.3.7.4 Deleting Profiles

Make sure you really want to delete a profile before you proceed. Once a profile has been deleted, the user-profile database will update to remove the profile from any of the user's available profiles. However, removing a profile will *not* update the user's last profile file. Deleting a profile that is currently in use by a user may result in unpredictable results.

To delete a profile, first bring up the Profile Catalog by choosing Profiles from under the View menu. Highlight the entry you want to delete from the catalog. To delete the entry, select Delete Profile from the Edit menu. A dialog box, similar to the one shown in Figure 29, will appear. To delete the profile, click Yes; to cancel the delete operation, click No.



dialog_popup

Are you sure you want to delete this profile?

Figure 29. Delete Profile Dialog

5.3.8 Viewing the Application Catalog

The Application Catalog provides a listing of the application icons delivered as part of the segments installed on the machine. As new segments are installed, a script automatically adds the segment’s icons into the Application Catalog. Therefore, the Security Manager does not provide any tools to manage this application list. Rather, for consistency, a set of administrative tools manages it that periodically reads the icon’s data files and repopulates the Application Catalog accordingly.

Follow the steps below to display the Application Catalog.

STEP 1: **Log in as the security administrator**. In the DII COE Login window (Figure 6), type secman in the Name field and press [RETURN].

STEP 2: **Enter the secman password**. In the DII COE Login window, type the secman password in the Password field and press [RETURN]. The Security Administration software appears.

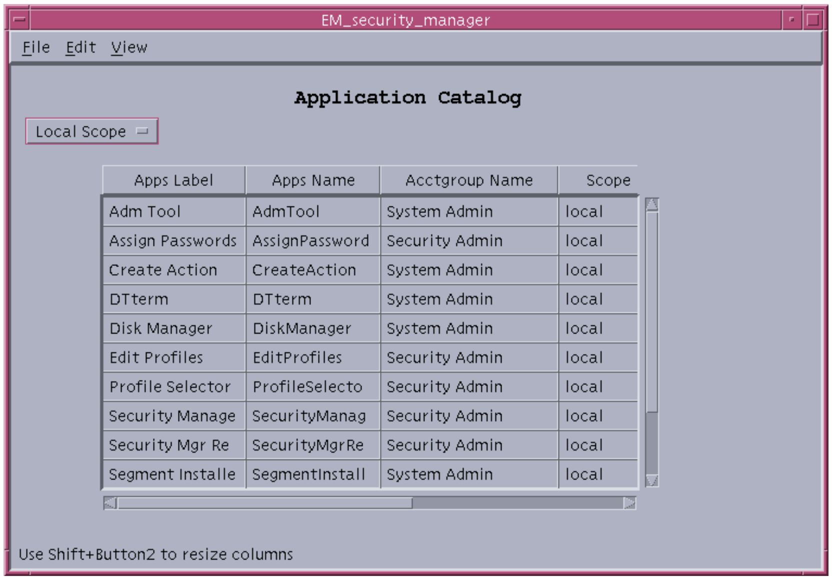
STEP 3: **Access the Application Manager**. Double-click the Application Manager icon on the CDE panel. The Application Manager window appears. For additional information about CDE, see the *TriTeal Enterprise Desktop User's Guide*.

STEP 4: **Open the `DII_APPS` folder**. Double-click the `DII_APPS` folder. The `Application Manager - DII_APPS` window appears.

STEP 5: **Open the `L:SSO_Default` folder**. Double-click the `L:SSO_Default` folder. The `Application Manager - L:SSO_Default` window appears.

STEP 6: **Open the Security Manager**. To open the Security Manager, double-click the `Security Manager` icon.

STEP 7: **Display the Application Catalog**. From the `View` pull-down menu, select `Applications`. A display appears, similar to that shown in Figure 30.



Application Catalog

Local Scope

Apps Label	Apps Name	Acctgroup Name	Scope
Adm Tool	AdmTool	System Admin	local
Assign Passwords	AssignPassword	Security Admin	local
Create Action	CreateAction	System Admin	local
DTterm	DTterm	System Admin	local
Disk Manager	DiskManager	System Admin	local
Edit Profiles	EditProfiles	Security Admin	local
Profile Selector	ProfileSelecto	Security Admin	local
Security Manage	SecurityManag	Security Admin	local
Security Mgr Re	SecurityMgrRe	Security Admin	local
Segment Installe	SegmentInstall	System Admin	local

Use Shift+Button2 to resize columns

Figure 30. Application Catalog

The Application Catalog contains the following fields:

Field Name	**Description**
`Apps Label`	The name used to uniquely identify this application. This name must be unique.
`Apps Name`	The full name of the application.
`Acctgroup Name`	The account group to which the application belongs.
`Scope`	The scope of the application. Currently, this is either local or global.
`Exec Path`	The fully qualified name of the executable (including path).
`Exec Arguments`	The arguments that need to be sent to the executable in order for it to run correctly.
`Icon`	The icon file name.

5.3.9 Maintaining UNIX Groups

The UNIX Group Catalog provides tools to administer UNIX group files or NIS equivalent. Use care when administering UNIX groups because they control much of the underlying access users have to DII applications. Follow the steps below to access the UNIX Group Catalog.

STEP 1: **Log in as the security administrator**. In the `DII COE Login` window (Figure 6), type `secman` in the `Name` field and press [`RETURN`].

STEP 2: **Enter the `secman` password**. In the `DII COE Login` window, type the `secman` password in the `Password` field and press [`RETURN`]. The Security Administration software appears.

STEP 3: **Access the Application Manager**. Double-click the `Application Manager` icon on the CDE panel. The `Application Manager` window appears. For additional information about CDE, see the *TriTeal Enterprise Desktop User's Guide*.

STEP 4: **Open the `DII_APPS` folder**. Double-click the `DII_APPS` folder. The `Application Manager - DII_APPS` window appears.

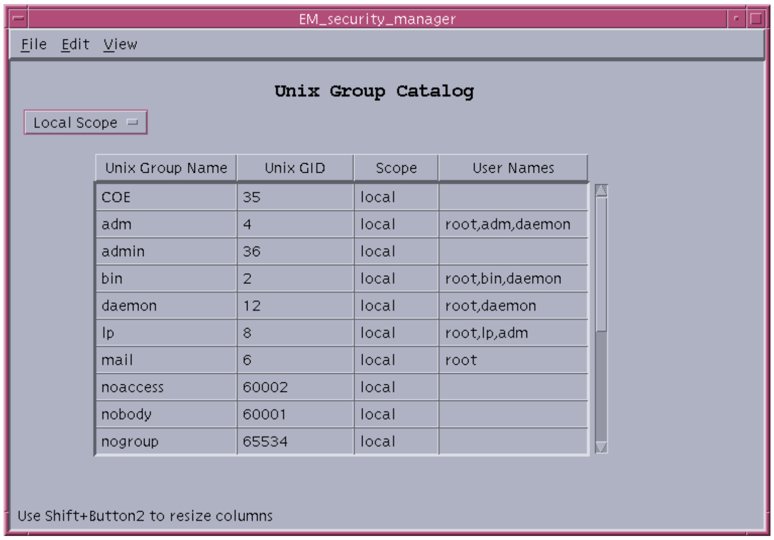
STEP 5: **Open the `L:SSO_Default` folder**. Double-click the `L:SSO_Default` folder. The `Application Manager - L:SSO_Default` window appears.

STEP 6: **Open the Security Manager**. To open the Security Manager, double-click the `Security Manager` icon.

STEP 7: **Display the UNIX Group Catalog**. From the `View` pull-down menu, select `UNIX Groups`. The UNIX Group Catalog appears.

5.3.9.1 UNIX Group Catalog

The UNIX Group Catalog provides a listing of the UNIX groups that have been defined in the selected scope (i.e., local, global, or both). To display the UNIX Group Catalog, choose `UNIX Groups` from the `View` pull-down menu. A display appears, similar to that shown in Figure 31.



Unix Group Catalog

Unix Group Name	Unix GID	Scope	User Names
COE	35	local	
adm	4	local	root,adm,daemon
admin	36	local	
bin	2	local	root,bin,daemon
daemon	12	local	root,daemon
lp	8	local	root,lp,adm
mail	6	local	root
noaccess	60002	local	
nobody	60001	local	
nogroup	65534	local	

Use Shift+Button2 to resize columns

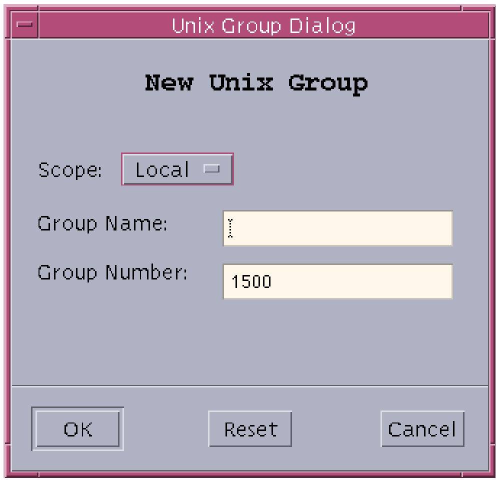
Figure 31. Unix Group Catalog

The UNIX Group Catalog contains the following fields:

Field Name	Description
`UNIX Group Name`	Name of the UNIX group. This should be distinct on a machine.
`UNIX GID`	The UNIX Group Identifier (GID).
`Scope`	The UNIX Group's scope (either local or global).
`User Names`	A comma delimited list of users currently assigned to the UNIX group.

5.3.9.2 Creating UNIX Groups

To create a new UNIX group, activate the UNIX Group Catalog by selecting `UNIX Groups` from under the `View` menu. Next, select `New UNIX Group` from under the `File` menu. A data entry screen appears, similar to the one shown in Figure 32.



Unix Group Dialog

New Unix Group

Scope: Local

Group Name:

Group Number: 1500

Figure 32. New Unix Group Dialog

Enter the following information into the fields provided:

`Scope`

Use the pull-down list to set the scope of the group. Currently, this is either `Local` or `Global`. A new local group enters into the local host's `/etc/group` file, and a global group enters into the appropriate NIS/NIS+ entry.

`Group Name`

Enter up to an 8-character alphanumeric field for the name of the group.

`Group Number`

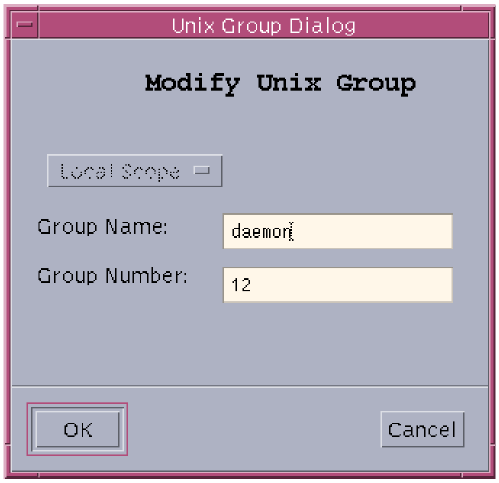
Assign the UNIX group ID. Security Manager automatically chooses the next available group ID based on the scope (configured in the Security Manager configuration file). You may choose to override the assigned number, but your selection must meet the minimum and maximum values established in the Security Manager configuration file.

You may use the same group number for more than one group name. However, group names must be unique, allowing to get around the limitation on the number of users that can be assigned to a group. The logical listing of group ownership is based on group names, but actual file and directory access by group permissions is derived from the group ID number.

Once you have entered the desired information, click `OK` to begin processing or `Cancel` to discard your changes.

5.3.9.3 Modifying UNIX Group Names

Security Manager allows you to change the name of a group but not the group number or the scope of the group. To modify a group name, activate the UNIX Group Catalog by selecting `UNIX Groups` from the `View` menu. Double-click the UNIX group entry that you want to modify. A `Modify UNIX Group` Dialog, similar to the one in Figure 33, appears. Type the new name of the UNIX group and click `OK` to make the change or `Cancel` to discard your change.



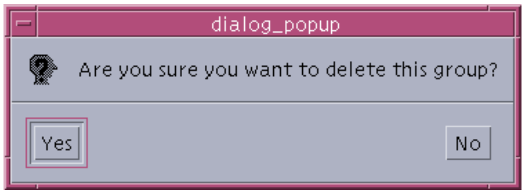
Group Name: daemon

Group Number: 12

Figure 33. Modify UNIX Group Dialog

5.3.9.4 Deleting UNIX Groups

Make sure you really want to delete a UNIX group before you proceed. To delete a UNIX group, first bring up the UNIX Group Catalog by choosing `UNIX Groups` from the `View` menu. Highlight the entry you want to delete from the catalog. To delete the entry, select `Delete UNIX Group` from the `Edit` menu. A dialog box appears, similar to the one shown in Figure 34. To delete the UNIX Group, click `Yes`; to cancel the delete operation, click `No`.



Are you sure you want to delete this group?

Figure 34. Delete Group Dialog

5.3.10 Changing the secman Password

Follow the steps below to change the secman password.

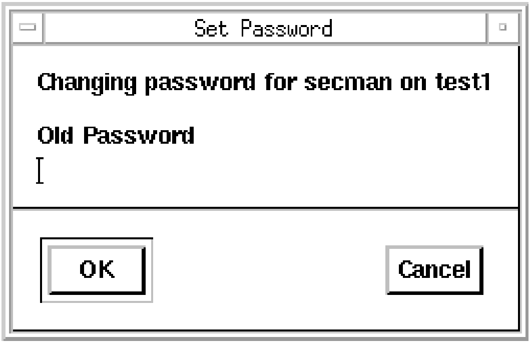
STEP 1: **Log in as the security administrator**. In the DII COE Login window (Figure 6), type secman in the Name field and press [RETURN].

STEP 2: **Enter the secman password**. In the DII COE Login window, type the secman password in the Password field and press [RETURN]. The Security Administration software appears.

STEP 3: **Access the Application Manager**. Double-click Application Manager on the Common Desktop Environment (CDE) panel. The Application Manager window appears. For additional information about CDE, see the *TriTeal Enterprise Desktop User's Guide*.

STEP 4: **Select the DII_TOOLS folder**. To open the Application Manager - DII_TOOLS folder, double-click the DII_TOOLS folder in the Application Manager window.

STEP 5: **Select the Chg Password icon**. To open the Set Password window (Figure 35), double-click Chg Password.



Changing password for secman on test1

Old Password

Figure 35. Set Password Window

STEP 6: **Enter the current secman password**. In the Old Password field, type the current secman password and click OK.

STEP 7: **Enter the new secman password**. The New Password window appears (Figure 36). In the Enter New Password field, type the new secman password and click OK.

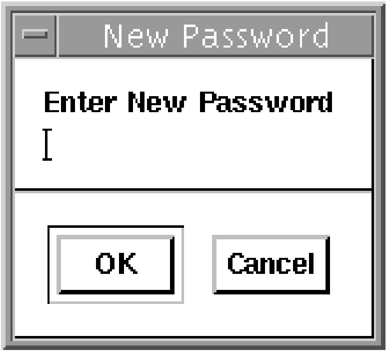


Figure 36. New Password Window

STEP 8: **Verify the new secman password**. The Verify New Password window appears. Type the new secman password and click OK.

STEP 9: **Acknowledge that the secman password has changed**. Click OK when the following message appears:

```
Your password has been successfully updated!
```

5.4 Related Processing

Section 5.4 applies to the Security Manager and not necessarily to the general Security Administration software.

Profile directives are a mechanism by which Security Manager can perform additional processing when a user is assigned or removed from a profile, or when an application is assigned or removed from a profile. The DII COE Kernel provides directives that a segment can specify during the installation process. These directives include actions to take when a user is created or deleted, and actions to be taken when a profile is added or deleted. The Security Manager also provides directives that a segment can choose to invoke when a user is assigned or unassigned to a profile and when an application is assigned or unassigned to a profile. These last two directives are not yet approved by Defense Information Systems Agency (DISA) for general use but were incorporated into the design of Security Manager to handle Security Manager's own processing needs as well as to provide an avenue for future growth.

5.4.1 Assign or Unassign Users to Profiles

Profile directives for user assignment to profiles are placed in the directory `/h/COE/data/UserProfileAssign`. Any executable file in the directory starting with an `A` will be invoked when a user is assigned to a profile. Any executable file in the directory starting with a `D` will be invoked when a user is removed from a profile. Both sets of scripts will be called with the following arguments, in order:

`User Number` The numeric user id of the account.

`User Name` The login name of the account.

`User Scope` The scope of the account (local or global).

`Profile Name` The name of the profile to which the user is being assigned or removed.

`Profile Scope` The scope of the profile (local or global).

> **NOTE**: A profile directive is provided to automatically add or delete a user from the NIS+ administration group when the user is assigned or unassigned from an administrative profile. Administrative profiles are listed in the file `/h/AcctGrps/SecAdm/admin/scripts/admin_profiles`. This file is modifiable by any user in the UNIX group `admin` and should be modified to contain a list of profiles that are to be assigned to users with System Administration duties.

5.4.2 Assign or Unassign Applications to Profiles

Profile directives for application assignment to profiles are placed in the directory `/h/COE/data/ProfileAppAssign`. Any executable file in the directory starting with an `A` will be invoked when an application is assigned to a profile. Any executable file in the directory starting with a `D` will be invoked when a user is removed from a profile. Both sets of scripts will be called with the following arguments, in order:

`Profile Name` The name of the profile to which the application is being assigned or removed.

`Profile Scope` The scope of the profile (local or global).

`Application ID` The ID of the application being assigned or removed.

5.5 Data Backup

Not applicable.

5.6 Error Recovery

For information on recovery from errors or malfunctions that occur during processing, see the error recovery guidelines in the *DII COE System Administrator’s Guide*.

This page intentionally left blank.